Blockchain Based Citizen-oriented Distributed Management System for Smart City

A Thesis

Submitted towards the Requirement for the Award of Degree of

Doctor of Philosophy

In

COMPUTER SCIENCE & ENGINEERING

Under the Faculty of Engineering & Technology

By

CHANDRA PRAKASH SINGH

ENROLLMENT NO.: 220101166

Under the Supervision of

Dr. ROHITA YAMAGANTI

2026

P.K. University

NH-27, Vill. Thanra (P.O.-DINARA), Shivpri (M.P.) India–473665

www.pkuniversity.edu.in

DECLARATION BY THE CANDIDATE

I declare that the thesis entitled **"Blockchain Based Citizen-oriented Distributed Management System for Smart City"** Is my own work conducted under the supervision of **Dr. ROHITA YAMAGANTI** at P.K. University, Shivpuri (M.P.) Approved by Research Degree Committee. I have put more than 240 days of attendance with Supervisor at the center.

I further declare that to the best of my knowledge the thesis does not contain my part of any work has been submitted for the award of any degree either in this University or in any other University Without proper citation.

Signature of the candidate

Date:……

Place:……..

CERTIFICATE OF THE SUPERVISOR

This is to certify that the work entitled **"Blockchain Based Citizen-oriented Distributed Management System for Smart City"** is a piece of research Work done by Shri **CHANDRA PRAKASH SINGH** Under Our Guidance and Supervision for the degree of Doctor of Philosophy of Computer Science & Engineering at P.K. University (M.P) India.

I certify that the candidate has put an attendance of more than 240 day with me. To the best of my knowledge and belief the thesis:

I –Embodies the work of the candidate himself/herself.

II – Has duly been completed.

III –Fulfill the requirement of the ordinance relating to the Ph.D. degree of the University.

Signature of the Co-Supervisor

Date:……..

Signature of the Supervisor

Date:……...

DrillBit

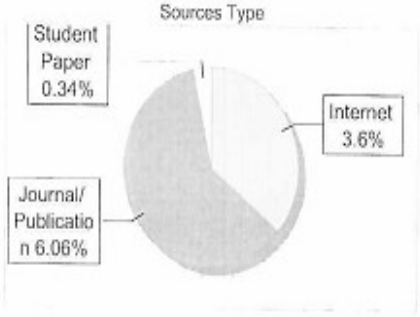
The Report is Generated by DrillBit Plagiarism Detection Software

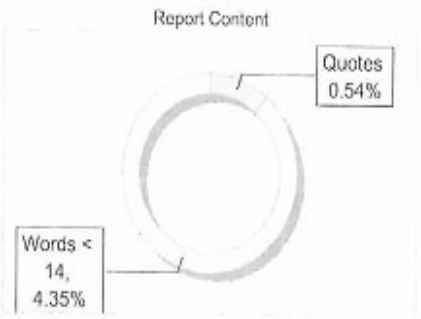
Submission Information

Author Name	Chandra Prakash Singh
Title	Blockchain based citizen-oriented distributed management system for smart city
Paper/Submission ID	5579004
Submitted by	library.pku@gmail.com
Submission Date	2026-05-01 14:43:59
Total Pages, Total Words	103, 23451
Document type	Thesis Chapter

Result Information

Similarity 10 %





Exclude Information

Quotes	Not Excluded
References/Bibliography	Not Excluded
Source: Excluded < 14 Words	Not Excluded
Excluded Source	0 %
Excluded Phrases	Not Excluded

Database Selection

Language	English
Student Papers	Yes
Journals & publishers	Yes
Internet or Web	Yes
Institution Repository	Yes

LIBRARIAN
P.K. University
Shivpuri (M.P.)

P.K.UNIVERSITY
SHIVPURI (M.P.)

University Established Under section 2f of UGC ACT 1956 Vide MP Government Act No 17 of 2015

Ref. No.:- PhD/PKU/2026/04/50/A Date: 17/04/2026

Pre – Ph.D. Submission Presentation Certificate

This is to certify that **Mr. Chandra Prakash Singh,** Enrollment No: **220101166,** research scholar under the supervision of **Dr. Rohita Yamaganti**, Department of **Computer Science & Engineering,** Faculty of **Engineering & Technology** has given his open Pre-Ph.D. submission presentation on the approved topic **"Blockchain Based Citizen-Oriented Distributed Management System for Smart City."** on Date **17/04/2026** at Time **02:00** PM in the P.K. University, Shivpuri (MP).

Dean Academic
P.K. University
Shivpuri (M.P.)

P.K.University
Shivpuri (M.P.)

Result - September-2023

Course:	Ph.D. in Computer Science & Engineering	Semester:	First Semester
Enrollment No:	220101166	Institute Name:	Faculty of Engineering & Technology
Student Name:	CHANDRA PRAKASH SINGH	Roll No:	222730080
Father's Name:	DAYA SHANKAR SINGH	Session:	2022-23

S.No.	Subject Code	Subject Name	Credit	Grade	Grade Point	Credit Point
1	PHD101	RESEARCH METHODOLOGY	4	B+	8	32
2	PHD102	COMPUTER SCIENCE & ENGINEERING	6	B+	8	48
3	PHD103	RESEARCH AND PUBLICATION ETHICS	2	A	9	18
		Total	12			98

SGPA:	98 / 12	8.17
CGPA:		8.17
Result:		Pass

* Grade in Repeat Examination



P.K.UNIVERSITY
SHIVPURI (M.P.)

University Established Under section 2F of UGC ACT 1956 Vide MP Government Act No17 of 2015

FORWARDING LETTER OF HEAD OF INSTITUTION

The Ph.D. thesis entitled **"Blockchain Based Citizen-oriented Distributed Management System for Smart City"** Submitted by Shri **CHANDRA PRAKASH SINGH** is forwarded to the university in six copies. The candidate has paid the necessary fees and there are no dues outstanding against him/her.

Name…… Seal……

Date: ……

Place:……...…

(Signature of Head of Institution where the

Candidate was registered for Ph.D degree)

Signature of the Supervisor Address:……..

Date: ……..

Place:……..…

P.K.UNIVERSITY
SHIVPURI (M.P.)

University Established Under section 2F of UGC ACT 1956 Vide MP Government Act No17 of 2015

COPYRIGHT TRANSFER CERTIFICATE

Title of the Thesis: **"Blockchain Based Citizen-oriented Distributed Management System for Smart City"**

Candidate's Name: **CHANDRA PRAKASH SINGH**

COPYRIGHT TRANSFER

The undersigned hereby assigns to the P.K. University, Shivpuri, (M.P. all copyrights that exist in and for the above thesis submitted for the award of the Ph.D. degree.

Date: …….

CHANDRA PRAKASH SINGH
Research Scholar (Com. Sci. & Engg.)

Note: However, the author may reproduce/publish or authorize others to reproduce, material extracted verbatim from the thesis or derivative of the thesis for authors personal use provided that the source and the University copyright notice are indic.

ACKNOWLEDGEMENT

The Acknowledgement of a research endeavor is an opportunity to express appreciation for the joint effort of those who have been sources of motivation and support, and who have contributed invaluable knowledge towards achieving success in the pursuit of knowledge. With utmost humility and pride, I reflect on the inspiring individuals who have propelled my work forward, and I am filled with immense pleasure, gratitude and thanks for their unwavering dedication.

First for most I would like to thank almighty god for preference, courage and strength bestowed on me to undertake this project.

For most, I extend my deepest appreciation gratitude to my esteemed Supervisor, **Dr. Rohita Yamaganti** Department of Computer Science & Engineering**,** P.K. University, Shivpuri, (M.P.)**.** I would also like to thanks Head of Department **Prof. (Dr.) Balveer Singh** and **Prof. (Dr.) Monika Tripathi,** Department of Computer Science & Engineering**,** P.K. University, Shivpuri, (M.P.) and Co-guide **Dr. Lokendra Singh Umrao,** Madan Mohan Malviya University of Technology, Gorakhpur without whom this work would not have come to fruition. His exceptional guidance, unwavering support kind cooperation and provision of a conductive work environmental have been invaluable beyond measure. I remain indebted to her instilling in me a relentless pursuit of excellence, a strong sense of honesty, and respect for ethical principles that govern our profession.

Furthermore, I extend my sincere thanks to the **Mr. Jagdeesh Prasad Sharma** Chancellor, P.K University Shivpuri (M.P) for providing the necessary infrastructure and facilities that were essential during my research work. My profound sense of gratitude, faith, also goes to **Prof. (Dr.) Mukesh Chansoriya,** Vice -Chancellor, P.K University Shivpuri (M.P) for his generous and valuable support throughout my research.

I take this pleasant opportunity to express my deep sense of gratitude and reverences to his holiness **Dr. Jitendra Kumar Mishra** Director; P.K University Shivpuri (M.P) for his constant encouragement and providing me with there quired facilities that enabled me to complete my project work.

Dr. Jitendra Malik Registrar, P.K University, Shivpuri (M.P.), who has inspired me with his encouraging guidance and support right from the beginning of this work in spite of his busy schedule. I am short of words to thank him for his affectionate behavior and patience throughout the duration of research work.

I express my gratitude to **Dr. Aiman Fatima,** Dean Academics, of P.K. University, Shivpuri, (M.P.)

I would also like to extend my gratitude to and deep appreciation to respected **Dr. Ashish Vishwakarma, Dr. Manish Kumar,** Incharge Ph.D. Cell, P.K. University, (M.P.)

I also express my gratitude to **Miss. Nisha Yadav,** Librarian of P.K University along with **Mr. Anand Kumar**, Assistant Librarian and other staff of P.K University. I am also thankful to Members of I.T. Cell of P.K. University.

I have no words to express my gratitude to my beloved parent's dear brother's and my wife for their love, support and constant encouragement during the entire course of my research work.

Last but not least I would like to honestly appreciate the fact that it is my pleasure to have an opportunity to pursue my higher education at P.K. University, Shivpuri (M.P). I owe my permanent debt towards it; this is having the special place in my heart for shaping my care.

I must also express my love and affection to my family members specially my beloved wife **Mrs. Kshama Singh** for her understanding and unwavering love during my research tenure, Lastly, I am highly grateful to God, the almighty, for giving me courage and strength to face the most difficult times of life and for answering my prayers in a special way. I remain grateful for all that I have achieved in my life thus far.

Date:

Place: **(Chandra Prakash Singh)**

CONTENTS

S.NO.	CHAPTER'S NAME	PARTICULARS	PAGE. NO.
1	CHAPTER 01	INTRODUCTION	01-26
2	CHAPTER 02	BLOCKCHAIN & SMARTCITY	27-51
3	CHAPTER 03	LITERATURE REVIEW	52-61
4	CHAPTER 04	RESEARCH METHODOLOGY	62-88
5	CHAPTER 05	RESULTS & ANALYSIS	89-95
6	CHAPTER 06	DISCUSSION	96-106
7	CHAPTER 07	CONCLUSION	107-113
8		REFERENCE	114-125
9		ANNEXURES	126-129

LIST OF TABLES

TABLE NO.	PARTICULARS	PAGE. NO.
1.1	Key Challenges in Smart City Governance and Blockchain Responses	**08-09**
2.1	Summary of Blockchain Features and Their Benefits in Smart City Governance	**38-39**
2.2	Comparison of Blockchain Types: Public vs Private vs Consortium	**40**
2.3	Blockchain Platforms for Smart Cities – Use Cases and Technical Suitability	**43-44**
2.4	Challenges and Potential Research Directions in Blockchain for Smart Cities	**45-46**
2.5	Key Domains and Technologies in Smart Cities	**49**
3.1	Research Gap Table	**59-61**
4.1	Metadata Schema for Citizen Transactions	**67**
4.2	Smart Contract Conditions and Execution Rules	**68**
4.3	Comparative Analysis of Consensus Mechanisms	**75**
4.4	Layer Description	**87**
4.5	Comparison of Global Smart City Reference Frameworks	**87**
5.1	Performance Metrics Summary	**93**
5.2	Security and Privacy Score Evaluation	**94**
6.1	Comparison of Traditional, Smart and Blockchain Based Smart City	**102**
6.2	Application scope in Smart Cities	**106**

LIST OF FIGURES

FIGURE NO.	PARTICULARS	PAGE. NO.
1.1	The Conceptual Framework Diagram	**21**
2.1	Evolution Timeline of Blockchain Technology	**29**
2.2	Basic Structure of a Blockchain Block	**33**
2.3	Workflow of a Blockchain Transaction	**35**
2.4	Access Control Differences in Blockchain Types	**41**
4.1	Proposed System Architecture	**54**
4.2	Architecture of Proposed BBCODMS	**65**
4.3	Transaction Flow from Citizen to Blockchain via Smart Contract	**66**
4.4	Flow Diagram of Mathematical Model	**69**
4.5	Flowchart for Proof of Work (PoW)	**70**
4.6	Flow Diagram of Mathematical Model for PoS	**71**
4.7	Flowchart for Proof of Work (PoW)	**72**
4.8	Visual Representation of PoW vs PoS	**72**
4.9	Mathematical Model for PBFT	**73**
4.10	Smart City Integrated Architecture	**76**
4.11	Citizen-Oriented Smart City Ecosystem	**80**
4.12	Smart City Layered Architecture	**86**
5.1	Transaction Throughput Comparison (Blockchain vs. Traditional DBMS)	**92**
5.2	Latency Analysis Across Multiple Nodes	**92**
5.3	User Trust Index Before and After Blockchain Integration	**93**
6.1	Blockchain Use Cases in Smart City Domains	**99**
6.2	Blockchain-Enhanced IoT Security Framework	**101**

LIST OF ABBREVIATIONS

- **AI** – Artificial Intelligence
- **API** – Application Programming Interface
- **CPS** – Cyber-Physical Systems
- **DApp** – Decentralized Application
- **DBMS** – Database Management System
- **DLT** – Distributed Ledger Technology
- **DPoS** – Delegated Proof of Stake
- **ERC** – Ethereum Request for Comment (e.g., ERC-20 token standard)
- **GPS** – Global Positioning System
- **ICT** – Information and Communication Technology
- **ICCC** – Integrated Command and Control Center
- **IoT** – Internet of Things
- **ITU-T** – International Telecommunication Union – Telecommunication Standardization Sector
- **KPI** – Key Performance Indicator
- **MoHUA** – Ministry of Housing and Urban Affairs (India)
- **ODE** – Open Digital Ecosystem
- **PBFT** – Practical Byzantine Fault Tolerance
- **PKI** – Public Key Infrastructure
- **PoA** – Proof of Authority
- **PoS** – Proof of Stake
- **PoW** – Proof of Work
- **RFID** – Radio-Frequency Identification
- **SACFA** – Smart Cities Application Framework Architecture
- **SC** – Smart Contract
- **SHA-256** – Secure Hash Algorithm 256-bit
- **TPS** – Transactions Per Second
- **UUID** – Universally Unique Identifier
- **ZKP** – Zero-Knowledge Proof

ABSTRACT

With the fast pace of urbanization comes an increased need for a more efficient and smarter way of urban management which should be aimed at citizens and their needs. As it stands today, even the most advanced centralized infrastructure faces various limitations when applied in smart cities: from lack of transparency and susceptibility to manipulation to data security concerns and very little citizen participation. Therefore, to foster sustainability in the implementation of smart city projects, there is a need for a new approach which could bridge the gap of mistrust between the government and the citizens. To that end, the present research aims to introduce the Blockchain-Based Citizen-Oriented Distributed Management System.

Blockchain technology with its inherent features, namely, distributed ledger, cryptography and a consensus protocol is one of the promising technologies that allows building an efficient and tamper-proof framework for data management and processing. With smart contracts implemented in the proposed system, automated solutions for digital identity, grievance redressal, utility service, licensing, and permissions are achieved. Moreover, the citizens gain control over their interactions with the smart contract and immutable logs increase the level of transparency.

The performance assessment of the proposed system will be based on a comparative analysis. Comparison with traditional centralized systems shows that there are numerous advancements made with regard to efficiency, effectiveness, and increased trust by the citizens. Moreover, the privacy concerns are managed effectively using decentralized identity management and permissioning of data.

Conclusions from the study indicate that the use of blockchain technology could revolutionize smart city governance as the governance becomes citizen-centric and minimizes any risks of manipulation with assurance of accountability in delivering services to the citizens. It is concluded that the implementation of a blockchain framework not only enhances efficiency but also builds the basis for democracy and transparency in urban governance systems.

CHAPTER-1

Introduction

1.1 Background

1.1.1 Rapid Urbanization and the Emergence of Smart Cities

The 21st century has seen a remarkable trend towards urbanization. The United Nations has reported that in 2020, more than 56 percent of the world's population lived in cities, and the number is projected to reach 70 percent in 2050. With the increasing expansion of cities to meet their burgeoning populations, problems arise in relation to infrastructure, energy, water, transportation, waste disposal, and public services. Thus, it becomes essential for the cities to develop intelligent and sustainable means of urban administration. This is where the idea of a smart city emerges [1].

Smart cities function based on the integration of ICT into urban infrastructure. Their primary objective is to leverage digital technologies to improve the standard of living of their inhabitants, automate administrative processes, and sustain development initiatives. Such urban environments utilize data gathering, processing, and automation technologies to manage everything from traffic signals and parking systems to energy systems and public security.

However, while most smart city projects boast sophisticated technology, few have achieved the expected results. The major reasons for failure include problems with centralization, data isolation, privacy breaches, and lack of trust among citizens. To bridge these gaps, there is need to rethink the architectural principles that underpin the development of smart cities [2].

1.1.2 Role of ICT in Improving Citizen Services

Information it is important to understand that the application of ICT in smart cities provides opportunities to digitize vital urban utilities such as healthcare services, education institutions, transportation networks, and energy distribution networks. Digitizing these utilities would result in generating a massive volume of data, and this data can then be used to forecast future trends and make informed decisions related to resource allocation and emergency responses.

ICT has been used for providing easier access to citizen services such as grievance redressal mechanisms, utility bills, identity verifications, and alerts regarding safety concerns by the use of apps on cell phones, web portals, and smart kiosks. The digital

infrastructure that connects government organizations and municipal corporations to citizens is provided by ICT infrastructure [3].

Nevertheless, the application of ICT within the context of cities comes with its own challenges, mainly in the area of data security and management. In most cases, centralized databases are used for storing and managing data generated by urban public utilities; therefore, data can be easily tampered with and even accessed without proper authorization. Moreover, ICT infrastructure lacks any mechanism for involving citizens.

1.1.3 Increasing Complexity and Volume of Urban Data and Service Demands

Modern In an urban setting, there is an ever-growing amount of data, coming from diverse sources like IoT sensors, GPS technology, surveillance cameras, smartphones, and smart meters. Such a large amount of data plays an important role in the day-to-day management of smart cities since it allows making decisions, doing predictive analysis, and monitoring.

However, managing data properly is not an easy job. Indeed, it involves the three main characteristics associated with big data: volume, variety, and velocity. Combining data from various systems (such as healthcare, transportation, utilities) without losing its accuracy and timeliness can be quite a difficult task. Furthermore, as people become increasingly reliant on new technologies, there are high expectations for municipalities to deliver seamless, personalized, and secure services [4].

Thus, citizens are expected to apply for various documents, pay taxes, make complaints, and stay informed using digital tools. However, there are also requirements that the provided services should be reliable, responsive, and resistant to attacks. The current situation does not correspond to those expectations because the provided services are not efficient enough.

The enormous amount of data, together with collaboration among multiple parties, demands a change in the way the provided services are managed [5].

1.1.4 Limitations of Traditional Centralized Management Systems

The current state of affairs regarding the management of smart cities relies heavily on IT infrastructure that operates in a centralized way. Centralized data bases and administrative systems empower a relatively small number of people who have been

authorized to do so, for instance, municipal authorities or national-level government agencies. Despite the positive aspects that a centralized architecture may bring,

first and foremost, it bears great vulnerabilities. A possible hack, disruption, or improper configuration of one component of the centralized system will affect the whole operation of city functions. Additionally, centralized data storage makes it very easy to target all data that has been accumulated there by malicious individuals. As a result, data breaches and leaks are rather common [6].

Secondly, centralization means lack of transparency. In many cases, citizens do not know where their data is stored, how it is processed, or whether it is ever disclosed somewhere else. Moreover, decision-making processes in centralized systems can be completely opaque to ordinary citizens.

Thirdly, such systems often lack efficiency due to bureaucracy and non-interoperability. Interdepartmental exchange of data is complicated, while the provision of services is slowed down by duplication of efforts and reliance on obsolete systems. Without a common and trusted system, issues such as data duplication, non-standard updates, and inefficient resource distribution arise.

In light of this scenario, it can be noted that the need for decentralization, transparency, and active participation from citizens becomes more relevant in urban administration. Thus, the ideal city of the future must have the capability to adapt to any changes, store urban information securely, and create a climate of trust and participation.

1.1.5 Rise of Blockchain as a Potential Enabler of Decentralized, Trustless and Transparent Systems

As a new technology, which was initially developed as the underlying technology of the digital currency Bitcoin, blockchain has proven itself as a revolutionary invention that could solve most of the issues raised in this discussion. The main features of blockchain technology include decentralization, consensus, cryptography, immutability, and smart contracts. All these factors ensure that the technology is perfectly suitable for application in smart cities.

The technology promotes the transition from centralized to decentralized mode of operation, where information can be entered by different parties and validated in a secure and transparent way.

The application of blockchain in smart cities could affect the following aspects:

- Management of identity: People would be able to control their identities in the digital world while reducing the dependence on centralized systems.
- Recording land and real estate: It could remove fraud and guarantee a true chain of ownership.
- Payment of utilities and payment of subsidies: Payments could be processed using smart contracts without any corruption.
- E-Government: Transactions could be recorded using blockchain technology and ensure secure voting and effective delivery of services.
- Data transfer and privacy: Secure transfer of data would be possible through blockchain encryption techniques and limited access ledgers.

Implementation of blockchain technology in the environment of smart city can help restore trust in digital governance, maintain integrity of information, and provide accountability for offered services. The major advantage of applying blockchain technology for governance is that it helps citizens gain power to participate actively in governance via codes.

Integration of blockchain technology and smart cities can be regarded as the key breakthroughs in urbanization and city management processes. Given the growing popularity of data-based smart cities, weaknesses of centralization became obvious. In such circumstances, blockchain becomes an important tool that allows achieving a citizen-centered approach and high efficiency at the same time. The present research is aimed at developing Blockchain-Based Citizen-Oriented Distributed Management System [8].

1.2 Motivation for the Research

With urbanization undergoing drastic changes, we have seen the emergence of the novel idea of smart cities, which can be said to be a paradigm shift in the way that urban environments are managed, services are delivered, and citizens interact in the smart city environment. Smart city environments rely on ICT, data analytics, and automation to ensure that the quality of life of the citizens improves and sustainable development is fostered. However, even with technological advancements, there are

certain very critical issues that have arisen with regard to the central management of smart cities, particularly issues relating to trust, security, transparency, and auditability.

1.2.1 Citizen Trust Deficit in Centralized Systems

Reasons for development one of the main factors contributing to the creation of the project has been the growing distrust of citizens with respect to centralized authorities. Traditionally, the process of implementing smart city projects was done using centralized databases, which do not provide any control over data processing for ordinary residents.

The consequence is a growing distrust and skepticism about the operation of both technology and government authorities. In addition, attempts at hacking databases and manipulation of urban services only worsen the level of distrust of citizens. Consequently, in the light of a growing use of big data in cities, it is crucial to implement measures to guarantee citizens' rights [9].

1.2.2 Security, Transparency, and Auditability Concerns

Another one of the main critical factors driving the need for research in this area is the fact that there are no well-designed security and auditing capabilities provided by existing smart city platforms. Using the centralized infrastructure makes these networks very vulnerable to cybersecurity breaches, insider attacks, and data manipulation. Indeed, once a hacker gains access to the centralized databases, he or she will be able to disrupt numerous services used by the citizens, including identity and health services, utilities and transportation data.

Furthermore, existing centralized systems do not provide transactional logging of services use, meaning that there will be no way to trace any kind of data manipulation done by a third party. Not only does this makes it impossible to hold anyone accountable, but also makes the transaction itself legally invalid, since no audit record has been provided.

Finally, there are some applications in smart cities, like voting and complaint management systems as well as decentralized utility billing services that require a decentralized mechanism of reaching an agreement and verifying transactions [10].

1.2.3 The Need for a Citizen-Empowering Distributed System

At citizens make up the core of every successful smart city. Unfortunately, conventional systems fail to offer true empowerment or participation of citizens within the process of city governance except for data contributions or feedback processes. The conventional smart city system is one which operates on the principles of provider governance wherein all services are controlled and regulated by governmental or municipal bodies.

The main motivation behind this study was the notion that citizens should have a say in the operation of the management and verification processes of their services. A true smart city must allow citizens to own their identities, verify their service credentials and city transactions, and be responsible for ensuring accountability using decentralized consensus mechanisms.

Citizen centric distributed management model transforms the conventional system by centering the citizen as a central character in the ecosystem. It would ensure that every interaction between the user and government services is transparent, independent of external influence and autonomous [11].

1.2.4 Blockchain as a Technological Enabler

The swift maturation of the blockchain technology is a highly plausible solution to the aforementioned problems. Initially intended for cryptocurrencies, such as Bitcoin, the blockchain evolved to become a generic decentralized ledger able to revolutionize industries well beyond the scope of the financial one. Intrinsic features of blockchain, which include immutability, decentralization, transparency, and verifiability, fully meet the requirements of a smart city.

The main value of blockchain lies in removing the reliance on the centralized trust model through facilitating trustless transactions between peers. Any transaction made using blockchain technology is timestamped, protected by cryptographic means, and recorded into a decentralized network in which changes are virtually impossible to implement. Using smart contracts, certain predefined conditions could be programmed to trigger actions automatically performed by services (utility bills generation, license renewals, public complaints handling, etc.) [12].

One additional and rather important feature of the blockchain technology is that it makes it possible to develop the self-sovereign identity systems, where personal information is controlled by a citizen and disclosed selectively when needed.

Finally, blockchain can provide a much-needed transparency and trust through enabling auditability of services provided. Such an approach is essential in critical fields, such as urban planning, public health, transport.

1.2.5 Strategic Alignment with Smart City Goals

Smart cities are designed to become inclusive, participatory, sustainable, and adaptive. Such aspirations can only be met through a technology infrastructure that embodies such traits. Blockchain technology, if integrated with the citizen-focused approach to urban planning, may become the catalyst for building a more democratic, resilient, and equitable framework of smart cities [13].

Therefore, this research suggests a distributed management system based on blockchain technology that improves service delivery and strengthens transparency, accountability, and citizen participation. This paper aims to illustrate the integration of blockchain technology into essential city services and the benefits that it brings in terms of data traceability, service verification, and decentralized governance.

The combination of blockchain and smart city planning remains underdeveloped. There are many conceptual and technical issues associated with the topic. This research contributes to the field by designing a scalable architecture and verifying its practical applicability in terms of performance metrics [14].

Table 1.1: Key Challenges in Smart City Governance and Blockchain Responses

Challenges in Conventional Smart City Systems	**Blockchain-Based Responses**
Centralized service control and data ownership	Decentralized, citizen-owned data models
Limited transparency and public accountability	Immutable, transparent ledger of actions
Data tampering and lack of verifiability	Cryptographically secured and auditable transactions

Weak cyber security due to centralized servers	Distributed ledger with no single point of failure
Manual or opaque service workflows	Smart contracts automate and validate service rules
Low citizen participation and trust	Peer-to-peer trustless mechanisms with self-verifiable identities
Difficulty in tracing service delivery and updates	Timestamped logs of all service interactions

1.3 Problem Statement

The idea of smart cities has been introduced as a revolutionary concept in urban planning, leveraging technology and internet connectivity to create efficient and effective urban environments. While there have been tremendous amounts of investment into ICT-enabled urban infrastructure, the core of the governance framework within the context of many smart city projects still relies on a centralized system. The centralized nature of such systems means that all vital decisions are made by a select few authorities or organizations, while all vital data is stored in one place.

1.3.1. Lack of Decentralized Citizen Engagement

One among other critical limitations of the current infrastructure in smart cities is a deficiency in active participation of the citizens in the decision-making process. Even if citizens have access to various online services that allow them to send complaints, request services, and give suggestions, such actions do not actually result in influencing governance policies in an easily verifiable manner.

In centralized infrastructure models, there is no opportunity for the interaction of the city authority and its citizenry to leave any kind of verifiable trace since all data will be stored in centralized servers. Consequently, the data can easily be altered, hidden, or modified, meaning that complaints about certain urban planning or service provision activities will remain unaddressed and will not result in any tangible action from the part of the administration [15]. Furthermore, citizen participation usually involves the use of surveying tools or public meetings, failing to harness the power of data analytics in real time.

Essentially, even though the idea behind smart cities is citizen-centered, the current lack of decentralization prevents it from achieving its purpose fully.

1.3.2. Vulnerability to Data Tampering and Service Manipulation

Centralized the systems in a smart city rely heavily on the use of centralized servers and their proprietary databases, which become single points of failure. The following vulnerabilities are two examples of how a smart city system becomes highly vulnerable due to centralized infrastructure:

- **Cyber security Threat**s: A centralized infrastructure is attractive to cyber threats, such as data theft, ransomware, or DoS attacks. A data breach may cause the theft of sensitive personal information from citizens, interruptions to vital services, and manipulation of decision-making algorithms. Because there is interconnectivity between various functions in the city, such as traffic management, waste management, water supply, and energy supply, a vulnerability in one node may affect multiple nodes.

- **Manipulation:** In the case where no cyber attack occurs in a centralized infrastructure, the possibility of manipulating the system by the administrators themselves remains. For example, performance reports of smart city services and feedback records can be manipulated to show more efficient operation and avoid accountability issues.

This may be the result of a corrupt administrator who wants to show better performance metrics to his superiors, thus earning promotions or raises. Likewise, an outsourced service provider may modify the performance metrics to avoid penalties for underperforming and to maximize profits [16].

1.3.3. Limited Audit Transparency and Privacy Assurance

Transparency is an essential element of effective governance, but centralized approaches frequently fall short of providing evidence-based, tamper-free audit trails. Most conventional audits depend on log files within the system that can be modified or erased by the administrators. Thus, both the citizenry and regulatory authorities must take the reporting party at their word instead of verifying the authenticity of the documents.

Regarding privacy, centralized repositories of personal data collect sensitive information such as identity credentials, financial records, behavior patterns, and

geolocational details in a way that may facilitate their exploitation. Privacy-by-design approaches are largely absent from these databases, meaning that the data gathered for one reason may be exploited for another without any consent from the affected individuals. These breaches contravene basic data protection protocols such as the GDPR and others.

Lastly, interdepartmental and interagency data exchanges between different municipal entities in smart cities are usually conducted in an opaque and undocumented fashion. Such practices create room for function creep, whereby data may be used for reasons other than its primary purpose [17].

1.3.4. The Governance Trust Gap

The cumulative impact of these limitations, such as centralized management, manipulation, and lack of an open auditing system, results in mistrust between residents and city authorities. Even though technology is used to boost efficiency, the lack of reliable and controllable systems of governance leads to a failure on the part of smart cities to meet their promise of transparency and citizen-oriented approach.

The consequences of this governance mistrust issue include the following:

- Lack of involvement in civic activities among citizens.
- Distrust of urban planning initiatives.
- Refusal to comply with rules as a result of perceived inequality.
- Mistrust in any further technology implementation efforts.

1.3.5. The Need for a Blockchain-Based Distributed Framework

Blockchain Technology provides an innovative approach to data recording, verification, and retrieval in relation to urban governance. The way blockchain is built is such that it generates a decentralized, tamper-proof and highly transparent database of all transactions which can then be replicated among various nodes. When it comes to smart cities' governance, blockchain technology allows for:

- The participation of citizens in the process of making decisions by means of a secure vote.

- A tamper-proof record-keeping system regarding service requests, progress reports and budget allocations.
- The creation of an automated identification and access system.
- The automated enforcement of urban governance policies via smart contracts.
- Data replication among various nodes.

1.3.6. Research Problem Definition

Despite with the known strengths of blockchain technology in areas like finance, logistics and healthcare, its application within the context of citizen-focused smart city governance is still limited. So far, most of the existing research work and pilot initiatives have concentrated only on some particular sectors, such as land records or electricity bills, but not on building a comprehensive citizen management solution.

In this regard, one may define the core research problem as follows:

What should be the architectural framework based on blockchain technology that will allow developing a citizen-driven smart city governance model providing transparency, auditability, privacy, and security against manipulations, and being scalable and flexible enough for different types of urban services?

Here it becomes necessary to consider the following issues:

- Urban governance architecture design.
- The integration with ICT/IoT infrastructure.
- Metadata and smart contracts for managing multiple services.
- Scalability, latency and security evaluation.

1.4 Research Objectives

The development process of smart cities has evolved from an infrastructure-focused approach to a citizen-focused governance approach, with the objective of ensuring effective provision of urban services, improving quality of life, and engaging citizens in the decision-making process. Nevertheless, the centralized model adopted by many smart city platforms is associated with certain constraints in terms of trust, transparency, and security of data. In light of this situation, blockchain technology becomes an ideal platform on which to develop solutions to overcome such constraints.

The research objectives for this study are defined as follows:

1.4.1 Objective 1: To Design a Blockchain-Based Distributed Framework Tailored for Smart City Management

This Objective entails developing a framework which will be built on a system architecture in which the blockchain is utilized as the underlying layer for smart city governance. It will comprise of multiple municipal public services such as digital identity, citizen complaints management system, licensing and permitting services, resource management services, and participative budgeting.

It entails adopting the decentralized architecture by replacing the current vulnerable central systems with a secure blockchain architecture that allows for consensus and ensures the integrity of data through the blockchain technology. The objective involves determining what type of blockchain (public or consortium or private) will be adopted, along with consensus mechanism, e.g., Proof of Authority and Delegated Proof of Stake.

Moreover, there is a need to determine how the municipal blockchain will integrate with the existing legacy systems and IoTs to enable smooth communication between legacy systems and blockchain platform.

1.4.2 Objective 2: To Create a Citizen-Centric Architecture That Ensures Secure Participation and Trust

At the essence of an intelligent city lies in its inhabitants. Unfortunately, the current systems tend to overlook citizens by turning them into mere consumers of services. The objective of this research is to transform that model by integrating citizen involvement in the governance blockchain layer.

Citizen-focused framework design will incorporate:

- Blockchain-based identity registration and authentication.
- People-specific permissioning to access city services.
- Flexible channels for providing feedback, voting, and approving services.
- Transparent process of recording issues and their resolution.

Blockchain allows for a data ownership model, whereby the individual has control over who has access to his data and how much access they have to it. Using cryptographic signatures and distributed identity systems like DIDs, the system can guarantee secure authentication without compromising the person's privacy.

In addition, this architecture will help build trust through transparent audit trails which are verifiable and unalterable by anyone. All citizen interactions with the government will be timestamped and cannot be changed.

1.4.3 Objective 3: To Develop Metadata Structures and Smart Contracts for Service Traceability and Automation

One of the most promising aspects of blockchain technology is the implementation of smart contracts – self-executing programs running on the blockchain. The current study will create smart contracts for the most commonly encountered transactions within smart cities. These include, but are not limited to, issuance of permits, verification of documents, processing of requests for services, budget allocation, dispute resolution, etc.

The design process will involve:

- Defining metadata schemas for each transaction.
- Programing business logic, workflows, and rules within the smart contracts.
- Implementing access control and verification procedures.
- Setting time-based and/or event-driven contract activation.

For example, when an individual requests permission to construct a building, the smart contract system will check the eligibility criteria, validate the attached documents, notify the concerned authority, and record the transaction in the ledger. On successful verification, a notification will be sent to the individual along with an official document.

This will help make the process streamlined, efficient, and will not require any audit processes because everything will be recorded on the blockchain. In addition, the metadata model will allow adaptability and scalability within different domains like health care, transportation, utilities, governance, etc.

1.4.4 Objective 4: To Evaluate the Proposed Model on Scalability, Security, and Performance Metrics

For our project to proceed, there is a need to perform an evaluation process that would assess the effectiveness and efficiency of our proposed blockchain solution. The evaluation process to be performed will involve the following performance metrics so that we can make a proper assessment of the system:

- Throughput: Number of transactions per second (TPS).
- Latency: Time taken to process the transactions.
- Scalability: Performance when the load increases (in terms of number of users, nodes, and services)
- Security: Potential attacks that the system can be subjected to, such as Sybil, 51% attack, double-spending, and so forth.
- Trust Score: Trust level from users of the system based on surveys and analytics.

To evaluate our proposed solution, a test environment (a simulated test environment or the creation of a prototype using testnet blockchain) will be used where our proposed solution will be compared to that of other centralized systems using the same workload.

Besides the evaluation above, we will also assess the cost of adopting blockchains, both computation, storage, and electricity costs, especially in implementations that use public blockchains and heavy verification algorithms.

1.5 Research Questions

To effectively address the problem and fulfil the stated objectives, this study is guided by a set of research questions. These questions form the backbone of the investigation and help in structuring the theoretical, technical, and empirical aspects of the research.

1.5.1 Research Question 1: How Can Blockchain Improve Transparency and Trust in Smart City Governance?

This question investigates the possibilities of blockchain technology to bring back the trust of the public through providing transparent services in urban areas. The concept of transparency in this case includes:

- Indelible documentation of activities performed by the municipal governments.

- Information on the performance of services available to the public.
- Evidence of citizens' involvement in the decision-making process.

In this study, it will be investigated how decentralization, immutable databases, and cryptographic validation systems may help prevent opaqueness and manipulation of government activities. Also, the effects of blockchain auditing on the public's views on smart cities will be assessed.

1.5.2 Research Question 2: What Architectural Model is Most Effective for a Citizen-Oriented Distributed Management System?

There are several options for implementing blockchain technology in smart cities – public or private, centralized or decentralized architecture, one or many nodes for decision making. This research is aimed at finding:

- An ideal architecture regarding the placement of nodes (citizen, government, third party).
- The most appropriate consensus algorithm (PoA, PBFT, DPoS, etc.).
- The way how data would be shared among citizen applications, smart contracts, and the city’s database.
- Compatibility with traditional IT systems and IoT devices.

The study aims to determine an architecture that balances decentralization with operational efficiency, ensuring both citizen control and system scalability

1.5.3 Research Question 3: How Do Smart Contracts Enhance Accountability in Urban Services?

This research will examine the impact of smart contracts in:

- Automating the delivery and validation of services.
- Implementing the rules of doing business and SLAs.
- Minimizing bureaucracy.
- Furnishing irrefutable evidence for service delivery to citizens.

In this regard, this research will focus on how these smart contracts could enable encoding the policy rules of the public sector, minimizing corruption, and increasing transparency of service delivery.

1.5.4 Research Question 4: What Are the Key Performance Benefits Over Traditional Models?

While blockchain holds theoretical promise, it is crucial to quantify its real-world advantages. This question focuses on:

- Comparing latency, throughput, and error rates with centralized systems.
- Evaluating operational costs (personnel, storage, computation).
- Measuring user satisfaction and trust levels.
- Assessing resilience to failure, manipulation, and cyberattacks.

The findings will provide evidence-based validation of the efficiency, robustness, and fairness of the proposed blockchain-based model.

1.6 Scope of the Study

This research project sets its boundaries very clearly by studying those areas where blockchain technology might have the ability to enhance the management of smart cities through better citizen services. Given the increasing complexities of modern urban living along with the necessity for transparent and efficient governance in the current scenario, this research aims to develop a blockchain-based framework to empower citizens in smart cities.

However, the study does not intend to address all possible aspects of smart city operations that might include things like transport systems, power grids, climate control systems, automated infrastructures, and more. Instead, it concentrates on improving governance and management of citizen services as it is clear that unless citizen services are managed efficiently and effectively, the full potential of smart cities cannot be harnessed.

The following subsections define the boundaries of the study in detail:

1.6.1 Citizen-Facing Services in Focus

In order to develop a blockchain framework, the following types of services need to be considered. The research will concentrate on services providing certain assistance to citizens and being vital to their functioning and the functioning of the city. Those services will include:

- **Citizen Registration and Digital Identification:** In connection with the research project, it is necessary to consider the development of blockchain solutions in order to enable a safe and secure registration process based on DID technology and ensure the right of citizens to control their personal data and regulate their disclosure according to applicable laws on data privacy.

- **Usage and Payments for Utilities:** As far as blockchain applications go, it will be possible to use this technology for monitoring usage and automatic generation and validation of bills associated with payment for certain services. Those services may include the supply of water or electricity and other sanitary services. This process will be controlled by smart contracts.

- **Complaints Management:** The next important function of the blockchain solution will be an automated complaints management process. In particular, all complaints submitted to relevant authorities will be recorded in the blockchain and protected from any deletion or modification.

- **Permits and Licenses:** The issuing and renewing process will be automated using smart contract management. It will streamline any paperwork related to permits and avoid human involvement.

By focusing on these types of services, the research will be able to create a more detailed and sophisticated system.

1.6.2 Blockchain Models Considered

This study evaluates the potential of two types of blockchain technologies for implementing services within smart cities:

- **Public Blockchain:** This type of blockchain consists of a permissionless and open system allowing any participant to become part of the blockchain. Although this type of technology is highly transparent and decentralized, there are certain issues

associated with scalability and latency. The public blockchain technology is regarded as being used in scenarios that require high transparency and citizen audits.

- **Consortium (Permissioned) Blockchains:** The consortium model of blockchain technology includes a group of trusted nodes who are responsible for verifying transactions and validating new blocks within the chain. Such technology allows greater scalability, privacy, and controllability as well as the ability to audit actions by citizens.

The research compares the strengths and limitations of both models in terms of performance, governance flexibility, and suitability for specific service domains

1.6.3 Use of Smart Contracts for Service Automation

Another key aspect in this research is the design and use of smart contracts: computer programs operating within blockchain technology that automate various steps in service delivery processes. In this study, smart contracts would have several applications, including:

- Automated verification and approval of service request applications based on eligibility requirements.
- Condition-based transaction automation, including issuance of license after payment is validated.
- Escalation of disputes after a period of time.
- Creation of time stamped entries for document submission and validation.

Through smart contracts, this study aims to minimize the inefficiencies associated with bureaucratic procedures, eliminating any human interference. The programming of smart contracts would take into account existing urban governance policies, while incorporating the efficiencies of blockchain technology.

In this research, smart contracts would be designed using existing languages like Solidity (Ethereum), or Chaincode (Hyperledger).

1.6.4 Simulation and Prototype Development for Evaluation

Considering the practical problems that may arise from deploying blockchain solutions within an actual smart urban environment (such as securing permissions, involving the local population, and creating adequate IT infrastructure), the current study will not

deploy any technology in a real-life situation but use simulation environments only. The scope of this research includes the following elements:

- Creation of a prototype application providing some citizen services that can be accessed through web/mobile interface.
- Deployment of blockchain nodes using Ethereum (testnet), Hyperledger Fabric, and other open-source blockchain technology solutions.
- Simulation of the communication between the platform and citizens regarding requests, submission of comments and proposals, and voting during different loads.

Collection and analysis of such performance measures as:

- Traffic (transactions per second)
- Latency in transactions
- Success rate of operations performed by smart contracts
- Scalability under concurrent requests
- Traceability of audit logs

Using simulation environments to test technological feasibility will allow avoiding the deployment of the developed technology in smart cities at the early stage of the project.

Moreover, a prototype can later be used to develop a sandbox for smart cities.

1.6.5 The Conceptual Framework

The Figure 1.1 shows proposed conceptual model which consists multiple layers that include:

- Users communicating with the system using apps, portals, and IoT devices.
- Service requests being handled by smart city applications.
- Blockchain providing transparency, security, and decentralization using smart contracts and digital identity solutions.
- Storage of data in a decentralized way using IPFS/cloud technology.
- Stream of live data provided by IoT infrastructure.
- Stakeholders cooperate on the basis of a trustless and safe.

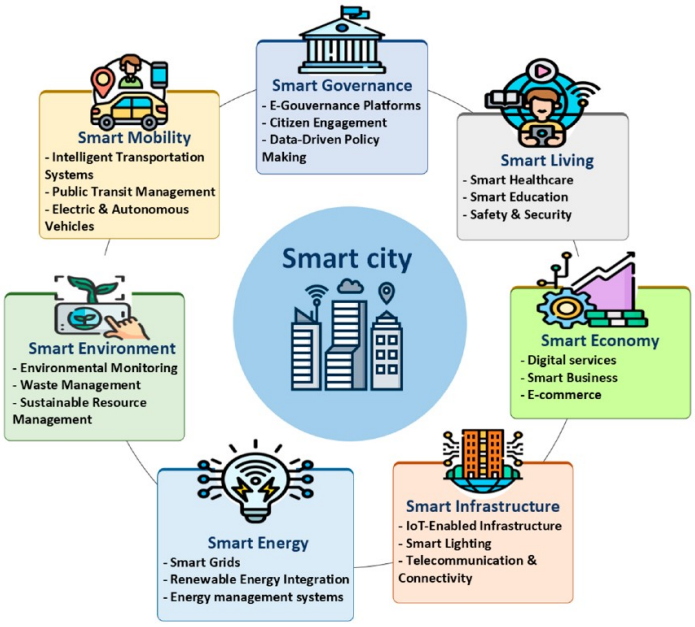


Figure 1.1: The Conceptual Framework Diagram

1.6.6 The flow from existing smart city challengesto a blockchain-enabled solution

The flowchart demonstrates how current smart cities problems such as centralization, non-transparency, and inefficiency have evolved into a blockchain technology-powered solution. The incorporation of decentralization, smart contracts, and digital identities helps create a trustworthy and transparent environment where service delivery and citizen engagement are improved significantly. Trust is replaced by transparency and automation with the help of blockchain technology.

1.6.7 Assumptions and Boundaries

To maintain feasibility and focus, the following assumptions are made:

- Citizens have access to basic digital infrastructure (smartphones, internet).
- City authorities are cooperative in implementing digital interfaces and publishing public APIs.
- Legal and data privacy implications are addressed at the conceptual design level, not actual legal integration.
- IoT device integration (e.g., sensors) is not a primary focus, though compatibility is considered for future scalability.

1.7 Structure of the Thesis

This Thesis consists of six logically organized chapters, where each subsequent chapter continues building on the ideas expressed in the preceding chapter. The organization of the thesis aims at providing the reader with a detailed understanding of the issue of creating an effective citizens' distributed management system based on blockchain technology. The analysis of different aspects of the thesis topic is carried out in each of the six chapters of the thesis, ranging from basic ideas and theories to implementation and results analysis.

1.7.1 Chapter 2: Blockchain and Smart City

The conceptual framework is discussed in Chapter 2, where a brief introduction to blockchain technology is made. The discussion of blockchain technology begins by looking at the history of this technology from its initial development in cryptocurrency networks to its current development as a versatile distributed ledger technology applicable in multiple sectors.

After defining the blockchain technology, the chapter proceeds to discuss the different types of blockchains, namely public, private, and consortium, as well as their respective uses and drawbacks. For example, public blockchains such as the Ethereum network are highly transparent and open, yet less scalable, while private blockchains provide better efficiencies, yet lack decentralization.

Next come the benefits of using blockchain technology, which include decentralization, immutability, auditability, fault tolerance, cryptography, and consensus. All these qualities represent the technical underpinnings for using the technology in the context of a smart city environment, with trust, accountability, and service traceability being crucial.

But blockchain is not without challenges, as the chapter highlights a number of problems associated with the technology. They include scalability problems due to low transaction throughput (transactions-per-second rate); energy inefficiencies of proof-of-work systems; data protection and privacy in public blockchains; interoperability of various blockchain networks; governance problems.

This chapter 3 zooms into smart cities to provide a definition of smart cities based on international guidelines, national policies, and research articles. According to this

chapter, smart cities are defined as environments where digital technologies and data-driven infrastructure are used to optimize the quality of life, utilize resources sustainably and effectively.

1.7.2 Chapter 3: Literature Review

In this chapter reviewed the literature studies clearly show that blockchain technology has the potential to transform cybersecurity in smart cities. Its decentralized structure, secure and permanent data storage, and trust-based system can improve existing security frameworks while supporting the development of future intelligent cities Overall, the literature about the blockchain, combined with technologies such as artificial intelligence, quantum computing, and optimization methods, could serve as a strong foundation for the smart cities of the future have been cited. Paper about emerging cyber threats and manage resources more efficiently also been reviewed.

1.7.3 Chapter 4: Research Methodology

Chapter 4 highlights the major contributions of this study, which include the Blockchain-Based Citizen-Oriented Distributed Management System for Smart Cities. This chapter is broken down into three segments.

Architecture

This segment outlines the architectural framework of the system. This includes the technological infrastructure applied (e.g., which blockchain platform, Ethereum and Hyperledger), role of the nodes, use of smart contracts, identity management framework, and the front-end citizen interface.

The transaction flow involves the interaction between a citizen and the system when requesting a certain service (such as birth certificate). It includes the process of request authentication and validation, recording, and fulfillment through the use of blockchain technology and smart contracts.

Metadata

This segment discusses the storage of information on citizen-service interactions in an organized manner through the use of metadata. The metadata field tables are provided along with the justification of the information captured.

The encryption methodologies, data validation, and consent management processes are also discussed.

This chapter also outlines the main components of smart cities: smart governance, smart energy, smart health, smart mobility, smart infrastructure, smart education, and smart environment. Each of these components is part of a web of relationships that depend on efficient information exchange, citizen participation, and effective service delivery.

Citizen is at the heart of smart cities since he/she stands to gain the most from such initiatives. The chapter focuses on the role of citizen-centric thinking, participative and inclusive governance, and the process of participative service delivery as well as decision-making in smart cities.

The basic structure of a smart city involves:

- The device layer (IoT sensors and actuators),
- The network layer (communication and transmission infrastructure),
- The data layer (cloud and edge storage), and
- The application layer (citizen services and dashboards).

A critical evaluation is made of the limitations in current architectures, especially the over-reliance on centralized cloud systems, which often lead to data silos, vulnerability to cyber-attacks, and lack of transparency. This sets the stage for integrating blockchain as a distributed and secure layer for managing data and citizen interactions in a decentralized fashion.

1.7.4 Chapter 5: Results & Analysis

Results and Analysis

This segment analyzes the performance of the proposed architecture through the use of key performance indicators:

- Transaction speed
- Gas/processing cost
- Security audit results
- Trust rating improvement

- Comparative latency analysis

The results are presented through graphs, performance tables, and system screenshots, validating the effectiveness of the solution.

1.7.5 Chapter 6: Discussion- Leveraging Blockchain Technology within Smart City Implementations

Chapter 6 describes link between theoretical understanding and the implementation of the blockchain technology in smart cities. This chapter elaborates the connection between the two by subdividing it into three sub-sections.

Blockchain Technology's Multi-faceted Role in Smart Cities

The first part is an overview of the ways that blockchain can help to solve the challenges faced in the development of smart cities. The examples include:

- The use of blockchain-powered digital identity to authenticate the citizens.
- The use of blockchain-based land registries to avoid conflicts with properties.
- The creation of blockchain-based e-voting systems to increase civic participation.
- Billing systems and public subsidies through smart contracts.
- Traffic and mobility management in cities with the aid of decentralized ledgers.
- Each of the use cases above shows how blockchain helps achieve efficiency, trust, data integrity, and automation.

Blockchain’s Role in Enhancing Smart City Security

In this section, cybersecurity advancements offered by blockchain are highlighted. The discussion begins with an analysis of blockchain as a means to offer secure data sharing platform, immutable records, and proper access controls. Smart contracts negate manual intervention points, hence minimizing chances of fraud.

Blockchain in disaster management, health crisis, and pandemics where transparency in data sharing is important is also discussed.

Blockchain Versus Traditional Technoligies: Comparative Analysis

Comparative analysis of blockchain systems and conventional technologies adopted in smart cities is carried out. This comparison is made on the basis of:

- Transparency
- Data integrity
- Service latency
- Trustworthiness
- Citizen autonomy
- Cost of infrastructure

This analysis forms a compelling argument for adopting blockchain as a core enabler of decentralized urban governance.

1.7.6 Chapter 7: Conclusion and Future Scope

In the last chapter, there is a recapitulation of the findings, highlighting the importance of blockchain for achieving smart city governance that is secure and oriented towards citizens.

There are limitations to the study, including issues related to scalability, governance of blockchain, and integration with existing legacy systems.

The chapter ends with suggestions for future research, which include:

- Integration with AI for predictive urban services,
- Interoperability among blockchains,
- Use of lightweight consensus mechanisms (e.g., Proof of Authority),
- Enhanced data privacy frameworks using zero-knowledge proofs (ZKPs).

CHAPTER-2

Blockchain and Smart City

2.1. Introduction to Blockchain Technology

Blockchain technology is a decentralized digital system used to record, store, and share data securely across multiple computers. Instead of relying on a single central authority such as a bank or government server, blockchain allows participants in a network to maintain a shared and tamper-resistant record of transactions.

The term “blockchain” comes from its structure: Blocks store data or transaction records and these blocks are connected in chronological order to form a chain.

Each block contains: Transaction data, timestamp and cryptographic hash of the previous block. This linking mechanism makes blockchain highly secure because altering one block would require changing all subsequent blocks across the network.

2.1.1. Overview of Distributed Ledger Technology (DLT)

At The basic principle of blockchain is underlain by a more comprehensive concept known as Distributed Ledger Technology (DLT). Distributed Ledger Technology is a digital ledger that records the transactions of asset ownership. The difference between the conventional method and the new innovation in technology is that, in DLT, transactions and their details are saved at multiple places simultaneously. DLT, unlike traditional data stores, does not have any central place or management function. On the contrary, it uses the technology of distributed ledgers where the ledger is spread across multiple computers in the network called nodes, and each node owns an exact copy of the ledger.

The main objective of DLT is that it is transparent, resilient, and resistant to any modifications. There is no central authority that runs the ledger, meaning that there is no single point of failure. All alterations made to the ledger are immediately reflected in all copies of the ledger in the network, depending on the consensus protocol used.

Distributed ledgers can either be permissioned or permissionless, where permissionless is an open platform, like Bitcoin and Ethereum [51].

2.1.2. Evolution of Blockchain: From Bitcoin to Multi-Industry Applications

Blockchain technology was first conceptualized in 2008 through the publication of the whitepaper *"Bitcoin: A Peer-to-Peer Electronic Cash System"* by an individual (or

group) under the pseudonym Satoshi Nakamoto. Figure 2.1 shows the beginning of what is now referred to as Blockchain 1.0, where the primary focus was on cryptocurrency and decentralized digital money.

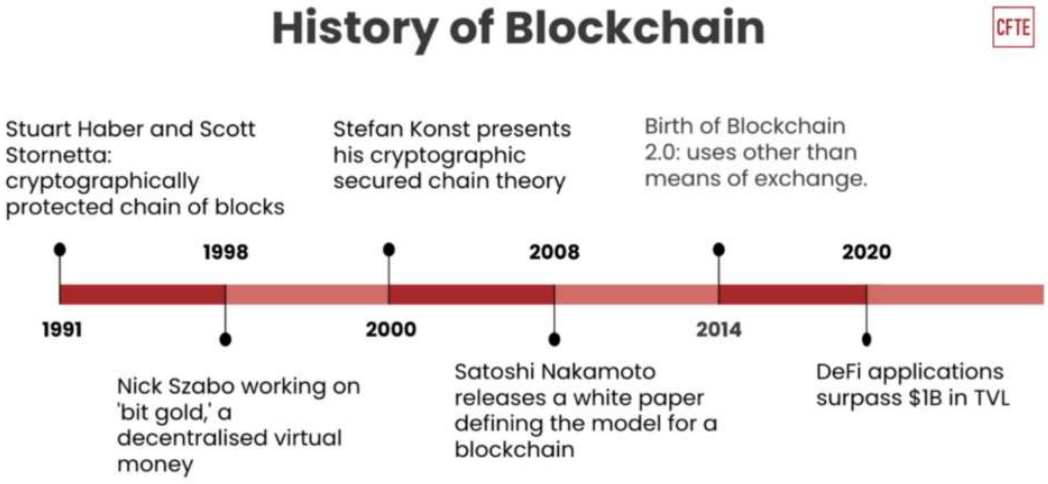


Figure 2.1: Evolution Timeline of Blockchain Technology

(Source: https://blog.cfte.education/the-history-of-blockchain-technology/)

2.1.3. Blockchain 1.0 – Digital Currency and Payments

The First Generation of Blockchain

First-generation blockchain technology was associated with the creation of cryptocurrencies such as Bitcoin. First generation of blockchain provided a platform through which financial transactions could be validated without the use of intermediaries. Blockchain 1.0 is characterized by proof-of-work (PoW). In this context, miners were required to solve mathematical puzzles as part of transaction validation.

Features of Blockchain 1.0

- Financial transactions were the main feature of first generation of blockchain.
- It promoted transparency and decentralization.
- It solved the problem of double-spending of digital currency.
- Mining was introduced.

Though it revolutionized financial sector, there are challenges associated with it.

2.1.4. Blockchain 2.0 – Smart Contracts and Decentralized Applications

The Limitations of Blockchain 1.0 were remedied with the advent of Blockchain 2.0, particularly with the launch of the Ethereum protocol in 2015. The Ethereum protocol allowed for the idea of smart contracts, which involve self-executing agreements based on the code. As a result, dApps could be developed within various application areas [52].

Key developments in Blockchain 2.0 include:

- Capability for programming via scripting languages such as Solidity.
- Smart contracts for development of dApps in areas such as finance, gaming, health care.
- Beyond cryptocurrencies – crowdfunding, identification, supply chains.
- Improved tokenization of assets via the ERC protocols (ERC-20, etc.).

Smart contracts allow for automation of complex operations and processes without direct human involvement and control.

2.1.5. Blockchain 3.0 – Scalability, Interoperability, and Enterprise Integration

The third-generation blockchain technology solves the problems related to scalability, interoperability, high energy consumption, and usability that emerged in previous generations. The main aim of this generation is to make blockchain technology more suitable for enterprise implementation and integration with legacy systems.

There are several well-known blockchain platforms from this generation, such as Hyperledger Fabric, Corda, and Quorum, allowing implementation of business and government agency-oriented blockchains (private/consortium ones).

Main characteristics of Blockchain 3.0:

- High transaction per second rate with improved consensus algorithms (PBFT, PoS).
- Cross-chain communication systems.
- Flexible permissioning system.

- Possibility to meet regulations and improve privacy (zero-knowledge proofs, etc.).

These innovations helped to lay the groundwork for blockchain usage in smart cities, healthcare industry, logistics, governance, and energy management.

2.1.6. Blockchain 4.0 – Industry 4.0 and Intelligent Automation

The concept of Blockchain 4.0 refers to the application of blockchain together with other upcoming trends such as AI, IoT, Big Data analytics, and edge computing, thus facilitating the emergence of autonomous systems. At this stage, there is the vision of blockchain as the underlying technology of CPS and Industry 4.0.

Drivers behind Blockchain 4.0 include:

- Instant exchange of information between IoT devices.
- Self-managing machine-to-machine communication.
- Smart contracts that utilize AI-based logic.
- Decentralized identity and access management solutions in smart environments.

In smart cities, Blockchain 4.0 may enable decentralized energy systems, smart traffic management, autonomous public transport, and e-government.

2.1.7. Importance of Blockchain in Decentralized Governance Systems

As As cities get smarter and interconnected, there is an immense increase in the amount of data generated by citizens in terms of quantity, speed, and variety. Conventional centralization methods face challenges such as data breach, lack of transparency, corruption, and inefficiencies caused by bureaucracy. This has led to the creation of mistrust between citizens and the government.

Blockchain provides an innovative approach in governance that guarantees:

- Transparency: Every transaction is timestamped and traceable using either a public or private blockchain network.
- Trust: Once the data is written, it cannot be altered without a consensus.
- Decentralization: There are no central points of failure or dependence on third parties.

- Accountability: The audit trail can be traced for every process and decision.
- Optimization: The implementation of smart contracts reduces paperwork and processes.

In citizen-oriented service delivery, blockchain can ensure that processes like citizen identity, voting, subsidies, land registry, and grievance handling are efficient, immutable, and easily accessible.

Additionally, blockchain integrated with IoT can provide a secure, tamper-proof method of storing data from sensors used in smart cities. For instance, smart meters and sensors for measuring pollution levels can automatically transmit data to the blockchain network for policymaking purposes [53].

2.2. Definition and Working Principle of Blockchain

A blockchain is a DLT platform that enables recording, storing, and transferring of digital information in an encrypted way without the involvement of any central authority. Essentially, blockchain is a chain of blocks that store verified information in digital form in the form of transactions. The blocks are interconnected using cryptography. In this regard, once the blocks are created and attached to the chain, they become tamper-proof because any change made to one of the blocks will necessitate making changes to other blocks that succeed it, which is impractical.

Conceptually, blockchain technology works on a P2P network where each participant keeps copies of the distributed ledger. The transactions on this platform are validated and recorded based on consensus algorithms, which are predefined rules followed by the nodes on how to validate transactions on the network. Once consensus is reached, a new block is added to the existing blockchain. Thus, the transaction data is replicated in the ledgers of each participating node [54]. The figure 2.2 depicts the basic structure of blockchain block.

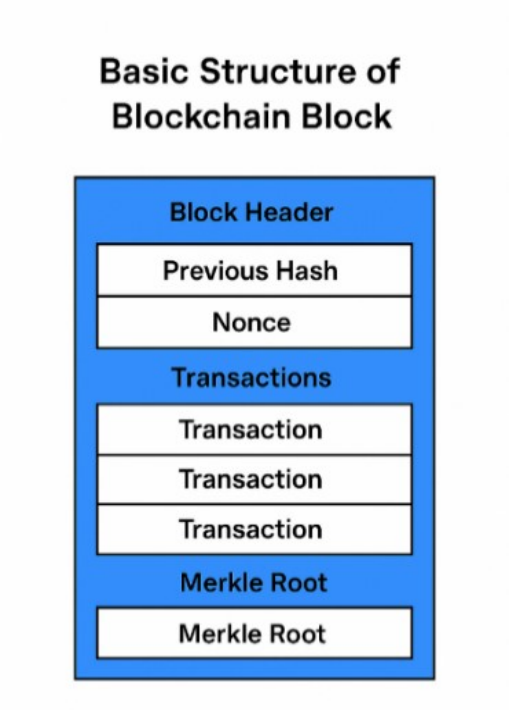


Figure 2.2: Basic Structure of a Blockchain Block

2.2.1. Core Components of Blockchain

In order to understand the working of blockchain, it becomes imperative to look into some basic building blocks of blockchain technology:

Blocks

Block is the core unit of data structure in blockchain technology. There are basically three main components in a block:

- Block Header – contains information like block number, timestamp, nonce, previous block hash.
- Txns List - List of valid transactions in the block.
- Merkle Root – single hash value made by hashing all transaction hashes in the block.

Hash

Hash is an alphanumeric output generated from input data of any length using a cryptographic function, for example, SHA-256. Some of the uses of hashes in blockchain are as follows:

- It maintains data integrity – slight changes in the input create a completely different hash.
- Hashes act as a digital signature for txns& blocks.
- Each block in blockchain contains a hash of the previous block.

Nonce

Nonce is an acronym of "number used once." It refers to a random or pseudo-random number included to a hashed block within the blockchain whose rehashing corresponds to certain criteria related to the degree of complexity. In a PoW blockchain, miners should discover a nonce so that hashing would generate a number of zeros at the beginning of the resulting value. This is known as mining and is essential for block validation [55].

Previous Hash

The previous hash is a value connecting the current block and the prior one and allowing building a chronologically linked chain of blocks. As such, it ensures the immutability of blockchain since any attempt to change a block will result in changing its hash and destroying its connection to other blocks.

Merkle Tree (Merkle Root)

The Merkle tree is a binary tree that summarizes large amounts of information. Within a blockchain block, transactions are summarized by hashing and combining pairs until obtaining the final hash (root). The root hash is incorporated into the header of a block and plays an important role in:

- Data integrity check;
- Fast transactions verification.

2.2.2. Step-by-Step: Transaction Validation and Consensus

The operation of blockchain follows a systematic sequence that ensures secure, decentralized transaction management. Below is a breakdown of how a transaction is initiated, validated, and confirmed in a blockchain network: The figure 2.3 depicts the Workflow of a Blockchain Transaction.

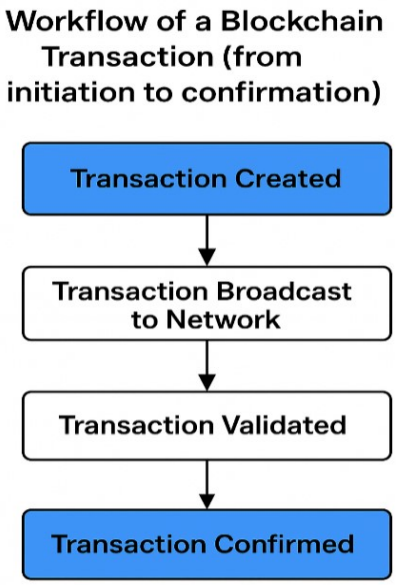


Figure 2.3: Workflow of a Blockchain Transaction

Step 1: Transaction Initiation

A blockchain transaction starts when one of the participants makes a request to log or exchange data on the blockchain ledger. For instance, a citizen in the blockchain-enabled smart city services platform could make a request to use a service, submit a complaint, or modify personal details. Such a transaction comprises crucial information like:

- Address of the sender and the receiver (public key of the sender and receiver)
- The data or digital asset in question
- Timestamp
- Digital signatures as proof of authenticity.

Step 2: Transaction Broadcast

After the transaction is signed, it is then broadcast to the entire decentralized network. Each of the participating nodes receives the transaction request and adds it to the list of unconfirmed transactions known as mempool.

Step 3: Transaction Verification

At this point, each node checks the validity of the transaction. It entails:

- Authentication of the digital signature.

- Authorization of the sender to conduct that particular transaction.
- Double-spend checking (in case of finance-related blockchains).

Step 4: Block Formation

An approved transaction is then packaged along with other approved transactions into a new block. The nodes or miners (based on the type of consensus used in the system) assemble a batch of transactions and proceed with the creation of a block. It involves [56].

- Organizing transactions in a Merkle Tree format.
- Determining the Merkle root.
- Specifying the metadata of the block (time stamp, the hash of the previous block, among others).

Step 5: Consensus Mechanism

The newly created block goes through a consensus procedure before being accepted into the network. Depending on the blockchain, different forms of consensus can be used such as:

- Proof of Work (PoW): where nodes engage in solving a difficult mathematical puzzle using their computing power and the first one to complete it sends the block out to be validated.
- Proof of Stake (PoS): nodes with higher stakes or token holdings become validators of the network.

PBFT, DPoS, Proof of Authority (PoA), etc.

The block becomes approved once consensus is achieved.

Step 6: Block Integration into Blockchain

Once a consensus process yields a valid block, it will be added to the blockchain. Every node will update their copy of the ledger.

Step 7: Transaction Confirmation

The transaction receives its first confirmation once the block is added to the chain. As subsequent blocks are added, more confirmations occur, strengthening the transaction's

permanence. For example, in Bitcoin, a transaction is considered highly secure after six confirmations.

2.3 Key Features and Strengths of Blockchain

The blockchain technology is a novel way of regulating the management of data because of its unique features. The features of the blockchain technology are important for the designing of the smart cities since they make sure that the smart city systems are both efficient and effective. This section will analyze some of the features of the blockchain technology.

2.3.1. Immutability

Immutability is the characteristic by which it becomes impossible to make changes to any kind of information after it is recorded on the blockchain system. Every single block is linked with a cryptographic hash of its preceding block, making the entire record immutable in nature. In a smart city scenario, immutability helps avoid fraudulent activities by preventing any tampering with important documentation like property rights.

2.3.2. Decentralization

The decentralized approach adopted in blockchain is completely different from that of centralized databases where there is a singular governing body managing all transactions. Decentralized systems have copies of ledgers stored on each node, hence reducing the possibility of a point of failure. This decentralized technology can help in the implementation of transparent governance for the smart city through data sharing among many parties involved.

2.3.3. Transparency and Auditability

With blockchain, all transactions will be visible to the right participants at all times and will be able to be audited in real time. The level of transparency that blockchain offers makes it possible for regulatory authorities and citizens to be able to keep track of how public funds are being used [57].

2.3.4. Security through Cryptographic Techniques

Blockchain technology uses cryptographic techniques to protect the data. The transactions are verified by the consensus algorithm and encrypted so that there is no

possibility of any intrusion or tampering with the data. In smart cities, especially when there are large volumes of highly confidential data being shared, such as personal or medical data, this becomes highly significant.

2.3.5. Smart Contracts for Automated Execution

These are digital agreements that become operational whenever certain conditions specified are fulfilled. Smart contracts minimize intermediation and enhance service delivery. In a smart city's parking system, the use of smart contracts would see the automatic freeing up of slots and deduction of money as soon as vehicles exit their designated parking zones.

2.3.6. Fault Tolerance and Trustlessness

Due to the fact that blockchain systems are decentralized, they exhibit high fault tolerance even when some nodes are either faulty or under attack. Also, blockchain systems allow for “trustless” environments where there is no need for an intermediary, such as a central authority, and prior knowledge of each other. This implies that smart cities will be able to provide their citizens with decentralized but reliable services.

The above characteristics of blockchain systems are the reasons why this technology will be helpful in developing smart cities. Below is a summary of how the characteristics of blockchain can help in the development of smart cities:

Table 2.1 – Summary of Blockchain Features and Their Benefits in Smart City Governance

Blockchain Feature	Description	Smart City Benefit
Immutability	Records cannot be changed once stored.	Prevents tampering of citizen data and public records.
Decentralization	Distributed ledger across multiple nodes.	Eliminates single point of failure; supports open governance.
Transparency & Auditability	All transactions visible and verifiable.	Enables real-time monitoring of public services and budget use.
Security through	Data secured by hashing and	Protects sensitive citizen and

Cryptography	encryption.	infrastructure data.
Smart Contracts	Self-executing coded agreements.	Automates service delivery (e.g., energy billing, permits).
Fault Tolerance &Trustlessness	Operates without central authority and is resistant to failure.	Supports reliable and citizen-driven systems without intermediaries

2.4 Types of Blockchain

Blockchain technology can be categorized into three major types based on their accessibility, governance, and control mechanisms: public, private, and consortium blockchains. Additionally, the distinction between permissioned and permissionlessblockchains adds another layer of classification, particularly relevant in institutional and government deployments like smart cities.

2.4.1. Public Blockchain

The public type of blockchain is an open-ended and decentralized network structure where everyone can freely join the network, take part in the consensus algorithm, and confirm transactions. Public blockchains are characterized by the use of trustless consensus algorithms (PoW or PoS) and complete transparency by enabling the auditability of transactions by any user [58].

Public blockchains can be deployed in contexts where transparency and openness are needed. Yet, they have limitations including lack of scalability, high energy usage (particularly PoW-based blockchains), and the absence of legal clarity, making them ill-suited for government-operated smart cities.

2.4.2. Private Blockchain

A private blockchain, which is also called a permissioned blockchain, is owned and operated by one entity. Access to it is limited, and only authorized members have the right to enter the network or take part in reaching a consensus. The Hyperledger Fabric created by the Linux Foundation is one of the most popular private blockchains.

Such blockchains are intended for internal use within an organization. This type of blockchain ensures that transactions will be processed efficiently and with the utmost

security. Private blockchains in smart cities could be used by the city government to maintain infrastructural and citizen databases.

2.4.3. Consortium Blockchain

A consortium blockchain is one that draws on the best aspects of the two other types. In this system, a select number of institutions/stakeholders run the blockchain network together. The system is governed collectively while being limited to specific individuals, unlike a strictly private blockchain. One real-life example of this type is the R3 Corda network which is applied within financial and government organizations.

Consortium blockchains are quite important in smart cities where inter-departmental cooperation is crucial, such as cooperation between transport, energy, and security departments of the city.

2.4.4. Permissioned vs Permissionless Blockchains

A further important categorization is that of permissionless and permissioned blockchains. In permissionless blockchains, typically public blockchains, anyone can take part in transactions and communicate with the distributed ledger. These blockchains are trustless and computationally intensive. On the other hand, permissioned blockchains limit access to certain users only. They are fast and energy-efficient.

Table 2.2: Comparison of Blockchain Types: Public vs Private vs Consortium

Feature	**Public Blockchain**	**Private Blockchain**	**Consortium Blockchain**
Access Control	Open to all	Restricted	Restricted to consortium members
Governance	Decentralized	Centralized	Federated
Consensus Participation	Anyone	Only authorized nodes	Consortium members
Speed & Scalability	Low	High	Moderate
Data Transparency	Full	Limited	Shared within onsortium
Example Platforms	Bitcoin, thereum	Hyperledger abric	R3 Corda
Use Case in Smart Cities	Public records	Internal admin records	Inter-agency ollaboration

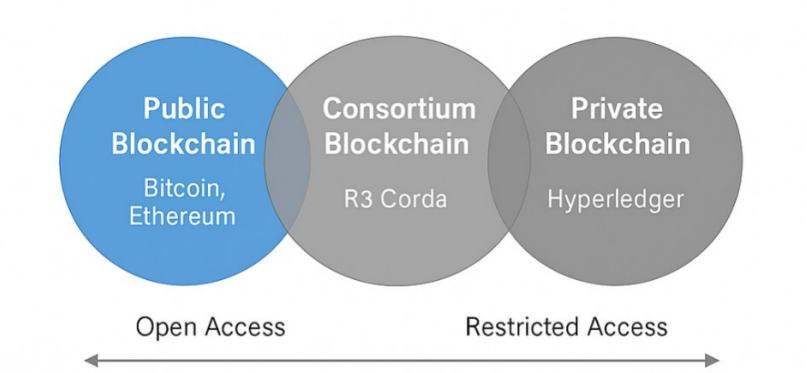


Figure 2.4: Access Control Differences in Blockchain Types

A diagram showing a Venn-style or layered schematic where Public, Private, and Consortium blockchains are shown along with arrows indicating open vs restricted access pathways.

2.5 Blockchain Platforms for Smart City Applications

For implementing the technology of blockchain in the smart city infrastructure, we need strong platforms that are scalable, modular, secure, and interoperable. The smart cities are comprised of different components such as energy grids, transportation networks, waste management, health care services, and governmental departments. Data is generated and consumed on a large scale by the smart cities. Hence, implementing blockchain in the smart city infrastructure will require the implementation of blockchain platforms that enable secure, tamper-resistant, and real-time interaction between the different entities [60].

Here, we discuss some prominent blockchain platforms being considered for smart cities: Ethereum, Hyperledger Fabric, Corda, Multichain, and Polygon/Quorum. Each platform has its own characteristics.

2.5.1 Ethereum

One of the most prominent examples of a public blockchain network is Ethereum. It offers smart contracts and dApps, which makes it a perfect solution for building open access systems such as e-governance, decentralized identification, and public procurement systems. The Turing-complete smart contract capability on Ethereum provides the possibility of developing personalized software applications.

Nevertheless, since Ethereum employs PoS and earlier PoW (before Ethereum 2.0), it frequently faces problems with transaction speed and gas fees. Still, Ethereum is currently considered the best option for implementing pilot and experimental solutions based on research findings.

2.5.2 Hyperledger Fabric

Designed by the Linux Foundation, Hyperledger Fabric is a permission-based distributed ledger technology with impressive levels of scalability, modularity, and advanced security solutions. The system allows the creation of private channels, ensuring data privacy among the participants of the transaction. Hence, Hyperledger Fabric becomes an ideal solution for managing supply chains, healthcare information, utilities accounting, and local government smart contracts.

Fabric differs from Ethereum by the absence of its own currency, which is considered a significant advantage when deploying in public institutions with strict regulatory requirements concerning the use of cryptocurrencies. Another feature is the ability to plug in any consensus protocol, as well as implement identity management functionality.

2.5.3 Corda

Corda was created by R3. It is yet another permissioned blockchain platform built specifically for enterprise purposes, particularly in the finance industry. Nevertheless, the capabilities of Corda have also been expanded into areas such as digital identity, land registry, and cross-entity collaboration in smart cities.

The point-to-point transfer of information in Corda ensures that data will only be shared with those who are supposed to receive it. This makes it an excellent choice for applications where privacy is a must, for example, police force collaboration and internal government communication. The notaries in Corda prevent double-spending and ensure the uniqueness of transactions.

2.5.4 Multichain

The Multichain platform is an adjustable blockchain network that allows one to develop and launch private blockchain applications easily. The ability to create custom assets, manage permissions, and use data streams makes Multichain an effective solution for

governments willing to utilize blockchain networks for asset management, document storage, and voting systems.

Multichain appears to be a great fit for smart cities that are just starting to implement blockchain technology because it is relatively easy to launch and requires fewer resources compared to other platforms. The detailed permissions management feature is another advantage that is essential in any government project.

2.5.5 Polygon / Quorum

Polygon (previously Matic) is a layer-2 scaling platform for Ethereum that aims to solve scalability issues within the Ethereum network. Polygon allows for rapid transactions at a low cost, as well as the ability to perform cross-chain actions. Therefore, it is suitable for applications that need high interaction frequencies, such as traffic management systems, IoT devices for recording sensor data, and utility payment services [61].

Quorum is an Ethereum-based permissioned version developed by JP Morgan and currently supported by ConsenSys. It combines the features of Ethereum smart contracts with privacy and performance improvements that suit enterprise-level operations. These platforms can be employed to develop hybrid smart city frameworks.

Table 2.3: Blockchain Platforms for Smart Cities – Use Cases and Technical Suitability

Platform	Type	Key Use Cases	Strengths	Limitations
Ethereum	Public	E-governance, Public records, Digital IDs	Mature ecosystem, Smart contracts	Scalability issues, High gas fees
Hyperledger Fabric	Permissioned	Utility billing, Health records, SCM	Private channels, Modular architecture	Complex setup, No native token
Corda	Permissioned	Inter-agency systems, Land	Point-to-point privacy,	Limited community

		registry	Notary services	adoption
Multichain	Permissioned	Voting, Public records, Asset tracking	Ease of use, Custom assets	Limited scalability and developer tools
Polygon / Quorum	Hybrid	IoT data, Utility payments, Mobility systems	Low-cost, Fast, Hybrid architecture	Quorum setup complexity, Interoperability

2.6 Open Challenges in Blockchain Adoption

Despite its revolutionary prospects, however, blockchain technology does have substantial issues—particularly when it comes to implementing it in the complicated networks that define a smart city. It is, thus, extremely important to realize the limitations inherent to blockchain technology within this context.

2.6.1 Scalability

Despite its revolutionary prospects, however, blockchain technology does have substantial issues—particularly when it comes to implementing it in the complicated networks that define a smart city. It is, thus, extremely important to realize the limitations inherent to blockchain technology within this context [62].

2.6.2 Interoperability

Smart cities consist of various systems that are governed by multiple departments and vendors. Incompatibility between blockchain systems may affect the exchange of data and workflow processes. Blockchain interconnection and interoperability technologies are in their infant stages, making it difficult to integrate blockchain into various service sectors such as healthcare, transportation, and utilities.

2.6.3 Energy Consumption

Although blockchain systems that use the proof-of-work algorithm (such as Bitcoin and Ethereum) have faced criticism for their energy consumption, there is now an increased interest in energy-efficient blockchain consensus algorithms (proof-of-stake, practical

Byzantine fault tolerance, or Raft). The environmental impact of blockchain remains a subject of controversy.

2.6.4 Regulatory and Legal Concerns

Introducing blockchain technology into government-regulated urban areas poses issues that must be addressed legally. Among the issues are those related to data localization, adherence to GDPR and other policies, as well as using blockchain technology as legal evidence.

2.6.5 Data Privacy vs. Transparency

Blockchain technology by its very nature is transparent, while data in smart cities, particularly citizen data, needs tight privacy policies. Balancing transparency and privacy is difficult. Technologies like zero-knowledge proofs (ZKP), ring signatures, and homomorphic encryption show promise, but they are highly complex and not yet implemented on a large scale.

2.6.6 Governance and Standardization

Finally, the lack of international governing principles for blockchain results in fragmented deployment processes. In the absence of an internationally agreed-upon approach to managing identity, deploying smart contracts, and managing consensus, initiatives such as smart cities may end up being isolated from other innovations.

Table 2.4: Challenges and Potential Research Directions in Blockchain for Smart Cities

Challenge	Description	Research/Development Direction
Scalability	Low TPS in public blockchains	Layer-2 solutions, Sharding, DAG-based ledgers
Interoperability	Lack of cross-chain standards	Cross-chain bridges, Interledger Protocols
Energy Consumption	High energy use in PoW systems	Adoption of PoS, PBFT, lightweight consensus
Regulatory Concerns	Legal status of blockchain	Government regulations, Legal

	records unclear	tech integrations
Data Privacy vs Transparency	Need for anonymity while maintaining audit trails	ZKPs, Differential Privacy, Selective Disclosure
Governance & Standardization	No unified framework for blockchain governance	ISO/IEEE standards, Consortium-led initiatives

2.7 Smart City: Introduction

In reality, in the contemporary era, the pace at which urbanization occurs is increasing at a rapid rate, altering the demographic landscape as well as the infrastructure of the earth. Since most of the world's population resides in urban areas, it becomes crucial to handle issues associated with resources, infrastructure, and facilities needed for individuals to have a healthy life and a high standard of living. It can be argued that conventional means of urban management, which involved centralized governance and disjointed service provision, are insufficient to solve contemporary urban problems.

It is in this background that the notion of smart cities has been proposed as one of the possible solutions to urban problems. Smart cities refer to a relatively new approach to urbanism where modern technology is used to enhance the management of urban infrastructure and amenities. Technologies that have been utilized for this purpose include the Internet of Things (IoT), Artificial Intelligence (AI), Blockchain, Big Data, GIS, Cloud Computing, and many others.

While the concept of a smart city may involve technology, it also encompasses the aspect of governance reform as well as citizen participation. The former serves as a facilitator; however, the end game is to deliver a higher quality of life, be inclusive, and promote sustainable development. Such an endeavor entails establishing mechanisms for citizen participation in governance, making evidence-based decisions, and providing timely delivery of services.

This chapter serves as a primer on smart cities. It reviews different definitions of smart cities from around the world, their key characteristics, and the underlying technologies that enable them. In addition, the chapter considers the objectives and principles of smart cities and a framework for aligning technologies with various urban sectors.

2.7.1 Definition of Smart Cities

The notion of a smart city has not been officially defined yet because the term is relative to the situation and changes as time goes by. Still, some organizations and governments have already come up with their own definitions of what a smart city is all about.

2.7.2 Definitions from Leading Organizations

According to International Telecommunication Union (ITU), a smart city is defined as:

"A smart innovative city that uses ICTs and other means to ensure that it provides improved quality of life, efficiency in urban operations and services, and competitiveness by ensuring its ability to meet the needs of the present and future generations considering the economic, social, environmental and also cultural dimensions."

According to ISO 37122 (Sustainable Cities and Communities -Indicators for Smart Cities):

"The adoption of digital technologies to improve the performance and well-being, decrease the cost and resource utilization, and better interact with its citizens."

According to World Bank, smart cities are characterized as:

"Cities that utilize digital technologies and data in their decision making, efficiency, and sustainability of urbanization."

According to the Smart Cities Mission of the Government of India, a smart city can be defined as:

"A city which provides core infrastructure and a sustainable environment, and gives its citizens a high quality of life with the help of smart solutions."

These definitions essentially reflect the basic concept behind the definition of smart cities – i.e., smart cities are essentially ecosystems driven by data and technology.

2.7.3 Common Characteristics of Smart Cities

In spite of differences in context, smart cities generally possess the following essential features:

- Technology Integration: Application of IoT, sensors, AI, cloud computing, and blockchain technology to build integrated urban systems.
- Data-Driven Governance: Analysis of real-time data for effective and informed governance.
- Citizen-Governance Approach: Involvement of citizens in participatory platforms, e-government services, and feedback mechanisms.
- Environmental Sustainability and Urban Greening: Encouragement of energy conservation, renewable energy, waste management, sustainable buildings, and climate adaptation measures.
- Integrated Infrastructures: Combination of physical infrastructures (transport, water supply), and digital infrastructures (broadband networks, cloud computing).
- Economic Innovation and Competitiveness: Facilitation of innovation ecosystems and digital entrepreneurship.

2.7.4 The Emphasis on Sustainability, Resilience, and Inclusivity

Sustainability, in terms of environmental, economic, and social aspects, is one of the key themes common in all smart cities. The cities use more than 75% of the total energy consumed globally and contribute significantly to greenhouse gas emissions. Smart cities are capable of adopting energy-efficient transportation, smart grids, water saving, and pollution reduction techniques.

Resilience in terms of climate change and increasing risks in cities is also one of the key principles. Smart cities are designed to anticipate any emergencies that might occur in terms of floods, epidemics, and cyber-attacks.

Citizenship and inclusiveness are also essential aspects. A smart city cannot be described as such if it is not inclusive. Technologies and services need to be available for everybody irrespective of their background.

Table 2.5: Key Domains and Technologies in Smart Cities

Smart City Domain	Description	Key Technologies Used
Smart Governance	E-governance, citizen portals, digital service delivery	Blockchain, Cloud, Web Portals, AI, Digital Identity
Smart Mobility	Traffic optimization, public transit, EV charging	IoT sensors, GPS, AI, Intelligent Transport Systems (ITS)
Smart Energy	Smart grids, renewable energy, demand-response systems	IoT, Smart Meters, AI, Blockchain (P2P energy trading)
Smart Water Management	Leak detection, smart metering, water quality monitoring	IoT, SCADA, GIS, Big Data Analytics
Smart Waste Management	Real-time bin tracking, route optimization	RFID, IoT, AI, GIS
Smart Health	Remote diagnostics, emergency response, health records	Telemedicine, AI, Wearables, Blockchain for data security
Smart Education	Digital classrooms, remote learning, learning analytics	EdTech platforms, AR/VR, Cloud, AI
Smart Safety & Security	Surveillance, crime prediction, disaster management	CCTV, AI, Drones, IoT, Blockchain for secure logs
Smart Environment	Air quality monitoring, noise detection, environmental alerts	IoT sensors, GIS, Machine Learning, Satellite Imaging
Smart Economy	Digital transactions, e-commerce, startup ecosystem	Fintech, Blockchain, AI, Digital Payment Platforms

2.8 Goals and Objectives of Smart Cities

A smart city is described as an urban environment characterized by use of technology, data, and innovations to overcome urbanization problems and sustain an

environmentally friendly development process. The basic principles of smart cities extend way beyond the incorporation of technology; instead, the primary objective involves bringing about transformational change within the governance structures and service provision frameworks. This chapter describes some of the basic principles guiding smart city projects.

2.8.1 Efficient Infrastructure Management

One of the main objectives of creating smart cities is the efficient utilization of infrastructure, including water supply, energy, transport systems, waste disposal, and other public utilities. Through IoT devices and sensors, smart cities can keep track of how their infrastructure operates, spot any faults, and perform preventive maintenance. Smart grids allow for dynamic management of energy supply depending on its demand. Moreover, smart water meters minimize water leakages and enhance its utilization. The proper management of infrastructure ensures financial savings and maximizes infrastructure life cycle.

2.8.2 Improved Quality of Life

The essence of every smart city lies in the intention of improving the welfare of its people. This involves ensuring that its citizens have quality healthcare services, live in secure environments, reside in affordable homes, enjoy fresh air and water, and make use of effective civic amenities. In this regard, digital technology can be used together with physical facilities to deliver healthcare services via telemedicine, enhance security using surveillance and emergency response mechanisms, and foster social participation through mobile applications and online governance portals.

2.8.3 Real-Time Service Delivery

A smart city seeks to change how services are provided in the city, moving away from fixed services that react to incidents to flexible services that operate in real time. Such services include transport, traffic control, waste management, and emergencies. Dynamic traffic lights will decrease congestion, while waste collection vehicles equipped with GPS will optimize their trips. Dashboards will enable the city administrators to track and correct any interruptions that occur during the delivery of the services.

2.8.4 Environmental Sustainability

Sustainability is one of the key components in making a smart city because of the increasing challenges posed by climate change and environmental degradation. Some of the aims of a sustainable city include reduction of carbon emissions, use of renewable sources of energy, creation of more green spaces, and sustainable urban planning. Energy efficient buildings, electric vehicles, and air quality sensors are some of the technologies that are vital for realizing these objectives.

2.8.5 Economic Development

Smart cities drive economic development that is innovation-driven through investments, entrepreneurship, and the creation of professional employment opportunities. Efficient processes are facilitated by digital technology, whereas innovations hubs, smart logistics, and connectivity corridors help make businesses more efficient. In addition, there are open data policies and private-public collaborations that stimulate business model innovation in fintech, mobility, health-tech, and green technology sectors.

2.8.6 Digital Inclusion and Transparency

One of the primary aims of a smart city should be to ensure digital equality by allowing all citizens, irrespective of their age, economic background, and level of literacy, access to various digital technologies. This would be achieved through making affordable digital technology available, user-friendly interfaces, and providing services in different languages. Moreover, transparency and accountability in the system of governance will be maintained through use of e-governance systems, blockchain ledgers, and feedback systems.

In essence, all of these objectives are interrelated and constitute an integral part of a smart city's strategy.

CHAPTER-3

Literature Review

Literature Review

Blockchain Technology has been found to be quite promising in terms of improving the security, privacy, and efficiency of the cyber-physical systems in smart cities. The authors in their work have highlighted a deep blockchain-based trustworthy privacy-preserving secured framework, known as DBTP2SF, that has been suggested as an answer to security issues that arise in terms of data communication and storage, through the combination of deep learning and the mechanism of distributed ledgers. It is evident from this that there has been a shift in the way of thinking in the literature and how AI and blockchains can be combined together to form an effective cybersecurity architecture.

Selvarajan and Mouratidis [19] have focused on the use of a quantum trust model alongside consultative transactions for securing healthcare data in smart cities. This is because this technology exploits the nature of blockchain to ensure immutability along with probabilistic security principles of quantum computing. Similarly, Aluvalu et al. [20] tackled the issue of wireless communications through privacy-enabled blockchain process mechanisms.

Selvarajan et al. [21] applied this concept in the IIoT domain, designing a light-weight blockchain-based security scheme driven by artificial intelligence for optimal operation under secure and private conditions. On the other hand, Mondal et al. [22] emphasized healthcare applications, suggesting a secured framework for storing electronic health records based on the blockchain principle to avoid any unauthorized access. This study highlights the potential of blockchain technology in regulated industries, offering data integrity and auditability.

Other scholars have made vital contributions to the fundamental concepts of multimedia and health data security through blockchain technology. For instance, Giri et al. [23] and Banotra et al. [24][25] developed multimedia-based security systems through blockchain, which can be used for data deduplication, authentication, and encryption purposes.

Within the domains of optimization and security on a network, optimization methods like Chameleon Swarm algorithm [26], Jellyfish Metaheuristic [27], and the attention-based LSTM approach for intrusion detection [28] were suggested for improving blockchain security. These optimization techniques have the potential to increase the

performance of the detection of anomalies and increase the efficiency of both proactive and reactive aspects of smart security systems. Other algorithms that were combined with blockchain systems include Adaboost algorithms [29] and Jaya Optimizer [30] for enhancing the intrusion detection capabilities in terms of increasing the number of detections and reducing false alarms.

The optimization method suggested by Brammya et al. [31] called the deer hunting optimization algorithm is used for improving decision-making processes in smart environments along with blockchain technology. Deep learning based on recurrent neural networks (RNN) has proven to be an efficient technique for intrusion detection [32] and has also been employed in cases involving blockchain systems.

Moreover, Wang et al. [33] enhanced the effectiveness of network intrusion detection through the integration of deep belief networks with kernel-based extreme learning machines. Selvarajan et al. [34] introduced SCBC, which refers to a smart city monitoring platform that integrates blockchain, IoT, and neuro-fuzzy methods to give a timely overview of city operations without compromising the confidentiality and integrity of data transactions.

Additionally, novel schemes for privacy-preserving authentication were developed by Rabie et al. [35]. In particular, the authors introduced a certificate-less aggregate signature authentication method for healthcare wearable networks based on the application of blockchain technology. Ghosh et al. [36] addressed the issue of detecting selfish nodes in IoT-MANETs through the application of the SVM technique and blockchain technology to avoid any manipulation of data transactions.

A more comprehensive assessment of blockchain-based security vulnerabilities and possible mitigation strategies was conducted by Saini et al. [37]. The authors highlighted the role of blockchain in addressing security limitations associated with conventional communication architectures. Moreover, Salah et al. [38] discussed the potential applications of blockchain in the agricultural sector through secure and transparent supply chains. Saleh [39] offered a proof-of-stake blockchain architecture that ensures sustainable use of energy resources.

A comprehensive review of the literature on blockchain security services has been done by Salman et al. [40]. They have grouped these services in categories of access control, identity management, and secure communication. This work summarized previous

findings and showed that blockchain could either substitute or enhance PKIs through a decentralized trust mechanism.

In 2022, Sanghami [67] have presented a ML-improved block chain consensus by TP-SC. In this paper, the future smart cities fully utilize blockchain technology in domains likes data safety, supply chain management, domination, data and energy management, urban management, transportation, and environmental monitoring, including emergency events. It uses a machine learning (ML) algorithm in the consensus protocol to attain effective leader election, to create new dynamic block creation process. Additionally, peer-forecast based verification mechanism was suggested to guarantee followers' honest evaluation of leaders' generated blocks. It provides high accuracy and low robustness.

In 2022, Uchani Gutierrez and Xu [68] have presented a block chain with smart contracts to secure property transactions in smart cities. Here, suggests a strategy to make acquisition, sale of real estate further equal, fair, rather being depending just on amount of money. Smart house able to classify its present owner by acting as IoT badge, after subject's identification validated, it provided full access to each services, or blocked and/or reported to authorities. Utilize of smart contracts in block chain to transfer ownership of smart home, which comprises inputs individuals interested in obtaining exact house, as outputs person who picked system depend on Smart City government's previously defined specifications. It provides high efficiency and low promptness index.

In 2021, Chiu and Meng [69] have presented an Edge TC-a PBFT block chain-depend ETC system for smart cities. Unlike most other block chain-depend ETC platforms utilize PoW or PoS, system employs PBFT for quicker performance. It compares system performance of Ethereum-depend with Hyper ledger-depend ETC in assessment. The outcomes show that when chain gets lengthy, the Ethereum-based system suffers from inefficiency, but the Hyper ledger-depend ETC maintain consistent time consumption through transactions. It provides high trustworthiness and low accuracy.

In 2023, Nayyer et al. [70] have presented novel framework for fraud detection in bit coin transactions through ensemble stacking method in smart cities. For data balancing, the suggested model employs ADASYN-TL (Adaptive synthetic + Tomek link)

balancing approach. Hyper parameter tuning is accomplished by the use of random search, grid search, Bayesian optimisation. The hyper parameters have important influence on the method's performance. It employed a stacking model that included DT, NB, K-NN, RF for classification. SHapley Additive explanation was employed to analyse stacking model's forecasts. It provides high promptness index and low efficiency.

In 2022, Saini et al. [71] have presented a. LSP: lightweight smart-contract-depend transaction prioritization system for smart medical care. It presents logical stateless transaction methods for various system entities with differing levels of confidence. Finally, method depend on private Ethereum beats the previous benchmark method regards utility in medical care scenario, compute cost by employing a simple prioritising mechanism. The collected findings show that the suggested approach is feasible in a real-time smart healthcare system. It provides high accuracy and low robustness.

In 2022, Deveci et al. [72] have presented decision support system for evaluating with prioritizing maintainable urban transportation in metaverse. Here, suggests hybrid decision-making framework for prioritising maintainable public transit in Metaverse in setting of q-rung ortho pair fuzzy set. To aggregate the qROF information, first q-rung ortho pair fuzzy generalised Dombi weighted aggregation operators, features were designed. Second, to determine objective, subjective weights of criteria, q-ROF information-depend technique depend on removal effects of conditions, stepwise weight assessment ratio analysis method was provided. It provides high promptness index and low efficiency.

In 2023, Tripathi et al. [73] have presented a new block chain and IoT-depend food traceability system for smart cities. A new BIOT-depend layered structure based on EOSIO was suggested in this study for effective food traceability. Here, determines appropriate traceability units to improve transparency, traceability before defining and implementing layered architecture on the Ethereum with EOSIO block chain platforms. The suggested EOSIO-based model's performance is assessed using consensus process's practicability, block production rate, throughput, and block confirmation time. It provides high trustworthiness and low accuracy.

In 2022, Wazid et al. [74] have presented Fortifying smart transportation security through public blockchain. This paper suggests PBSCF-ITS which ensures access control and key management between vehicles, between roadside units, and between roadside units and cloud servers. It examine PBSCF-ITS's security to demonstrate its resistance to many forms of potential assaults. Also, the performance of PBSCF-ITS have been compared to that of other relevant competing systems. The results show that PBSCF-ITS shows outperforms the current ones. Also, a pragmatic research of PBSCF-ITS being done to examine its impact on key network-related performance factors like as the number of mined blocks and transactions per block. It attains higher promptness index, lower robustness.

In 2021, Kumar.,et al., [75] have presented trust worthy privacy-preserving secured framework for maintainable smart cities by leveraging block chain and ML. Here, suggested two-tier privacy module along with an intrusion detection module. A blockchain reputation system based on addresses is designed in trustworthiness module. Dual-level privacy module transforms data into novel reduced shape to thwart inference, poisoning attempts by applying Principal Component Analysis (PCA) and improved Proof of Work method depend on blockchain simultaneously. An optimized gradient tree boosting technique is implemented in the intrusion detection module. It provides high accuracy and low recall.

In 2021, Kumar, R.,et al., [76] have presented privacy-preserving-depend secure framework utilizing block chain-enabled DL in cooperative intellectual transport system. In this paper suggested architecture uses deep learning modules and blockchain technology to give two levels of security and anonymity. A DL module was constructed that integrates the LSTM-AE method for encoding C-ITS data into novel format, thereby guarding against inference attacks. Two datasets, ToN-IoT and CICIDS-2017 that are accessible to the public are used to further validate and test the system. It provides higher accuracy, lower specificity.

In 2021, Kumar.,et al., [77] have presented block chain with DL framework for privacy-preserved threat intellect in industrial IoT. Here, suggested a novel P2TIF to detect cyber threats in IIoT contexts and safeguard sensitive data. Initially, a blockchain module that can be expanded and offers secure IIoT data transport while guarding against data poisoning. Secondly, DL module called deep variational auto encoder (DVAE) that protects against inference attacks through rearranging real data into a

secure format. Then, a threat detection system employs the encoded data to identify dangerous patterns in IIoT environments by utilizing attention-depend deep gated recurrent neural network. It provides high precision and high false rate.

In 2023, Ahamad.,et al., [78] have presented dual level block chain-depend privacy preservation framework in IoT by heuristic fusion mechanism-assisted DL architecture. In this work suggested novel method to IoT-based privacy preservation, embraced by blockchain technology, is being developed to offer increased security while minimizing the usage of resources. Deep learning is the method used to achieve two degrees of data privacy. As a result, encrypted data was sent to data decryption procedure, where it is processed by the auto encoder's decoder to recreate the original data. It attains higher recall, lower specificity.

In 2022, Hamouda.,et al., [79] have presented privacy-preserving secure framework utilizing blockchain-allowed federated DL for Industrial IoT. This study suggested a unique privacy-preserving secure framework (PPSS) with enhanced privacy, verifiability, and transparency was built on utilization of blockchain-allowed FL. In order to protect client updates' privacy, initial step utilizes differentially private training of stochastic gradient descent, second stage utilizes the PoFDL protocol to validate, add novel blocks to blockchain that contain models. It provides higher accuracy, lower precision.

In 2023, Om Kumar.,et al., [80] have presented securing medical care data through blockchain enabled collaborative ML. Here, suggested utilizing the Zero Knowledge Proof (ZKP) technique, new scalable block chain architecture was suggested to guarantee data integrity, secure data transmission. Next, BDSDT interfaces by Ethereum smart contract to handle data safety concerns with off-chain storage IPFS to address issues with data storage costs. To detect intrusions in HS network, deep learning architecture is designed utilizing verified data. The latter creates efficient IDS by combining Bi-LSTM with Deep Sparse Auto Encoder. It provides highF1-score and low precision.

From all these papers, one thing is clearly evident: blockchain is set to revolutionize how smart cities handle cybersecurity issues. Through its distributed trust, immutable data record keeping, and decentralized governance model, blockchain is not only able to enhance security measures currently in place but also lay the foundations for future

intelligent cities. Moreover, the combination of machine learning with blockchain provides smart cities with advanced means to detect new security threats and optimize resources. Although scaling, interoperability, and energy concerns exist in this technology, current research shows great interest in overcoming them by employing different solutions.

Lastly, the variety of application areas such as health, multimedia, industry, agriculture, and public utilities shows the strength of blockchain. In summary, the reviewed literature indicates that blockchain can be the backbone of future smart cities, especially with the help of artificial intelligence, quantum computing, and optimization techniques.

Table 3.1 describes the research gap with contributions and key focus.

Table 3.1: Research Gap Table

Ref. No.	Authors / Title	Key Focus	Contribution	Identified Research Gap
[40]	Salman et al., 2019 – Security services using blockchains	Survey of blockchain-based security services	Comprehensive classification of blockchain-based access control, authentication, and privacy-preserving models	Lack of lightweight blockchain solutions suited for real-time smart city services
[41]	Sandhu et al., 1996 – Role-based access control (RBAC) models	Role-based access control in computing environments	Established RBAC model for secure access management	RBAC needs integration with decentralized identity systems in smart cities
[42]	SmartSantander Facility, 2018	Real-world smart city IoT testbed	Provided infrastructure for IoT experimentation in urban settings	Lacks integration with blockchain for decentralized, tamper-proof IoT management

[43]	Sasaki, 2010 – Creative city theory	Cultural creativity and inclusion in urban planning	Proposed socio-cultural regeneration strategies	Does not address secure digital infrastructure for citizen engagement
[44]	Schwartz et al., 2014 – Ripple consensus algorithm	Ripple protocol for decentralized consensus	Introduced a scalable, efficient consensus algorithm	Not fully explored in public blockchain environments for citizen-oriented applications
[45]	Sengupta et al., 2020 – Survey on IoT/IIoT security with blockchain	Review of attacks, vulnerabilities, and blockchain solutions	Detailed taxonomy of IoT threats and blockchain countermeasures	Few studies address end-to-end integration of blockchain with large-scale IIoT platforms
[46]	Shamir, 1985 – Identity-based cryptosystems	Introduction of identity-based encryption and signatures	Pioneered cryptographic techniques for secure identity management	Integration of identity-based encryption with blockchain for smart city authentication systems is underexplored
[47]	Sharma & Park, 2018 – Hybrid network architecture for smart cities	Blockchain-integrated architecture for secure communication	Presented a hybrid framework combining cloud and edge networks	Evaluation in real-world smart city scenarios is limited
[48]	Sharma et al., 2018 – Fog-	IoT security using blockchain	Developed architecture to	Scalability and latency

	based blockchain cloud architecture	and fog computing	process IoT data securely at the edge	optimization in large urban deployments not fully addressed
[49]	Sharma et al., 2019 – Blockchain in automotive industry	Blockchain for securing smart vehicles and connected infrastructure	Demonstrated benefits of decentralization in vehicular networks	Lacks integration with city-wide data governance platforms
[50]	Sheikh et al., 2020 – Secured energy trading using blockchain	Energy market transactions secured through Byzantine consensus	Proposed secure trading model using resilient consensus mechanism	Energy trading systems with user privacy and real-time adaptation in smart grids are underdeveloped

CHAPTER-4

Research Methodology

Introduction

Smart cities are an initiative to respond to the problems that arise from rapid urbanization through the integration of digital technology into the infrastructure and services of a city. The current smart city governance model, however, poses many limitations. First, it is centralized. Citizen services under such a model are controlled by one or more agencies, resulting in bottlenecks, inefficiencies, and a lack of citizen control. Second, the data collection system in the current city management process is fragmented and inefficient. In most cases, different government agencies operate independently, which means that there is redundancy in record-keeping and information sharing, as well as a lack of data interoperability. Third, there is a lack of citizen trust in city authorities. Citizens are not aware of the process involved in the delivery of public services or the possible presence of favoritism in the processing of requests.

Blockchain technology offers a radical innovation to address these issues. With the integration of distributed ledger technology, consensus algorithms, and smart contracts, blockchain enables transactions that are transparent, secure, and trustless, making it perfect for providing citizen-centric services. The development of a blockchain-powered distributed citizen service management platform would lead to greater transparency, accountability, audibility, and transaction integrity. Citizens will be able to create new service requests, monitor the status of the request in real time, and access immutable and verifiable transaction records without compromising on their privacy.

The main reason behind proposing this solution is to provide citizens with more power, enhance operational efficiency, improve security, and ensure resilience in the provision of services. Smart contract implementation will minimize human involvement and bias, automate service workflow conditions, and drastically decrease service delivery time. Additionally, blockchain technology uses cryptography to ensure that citizens' data remains secure and accessible only by authorized parties.

Objectives of the Proposed Solution:

- To create a modular and decentralized architecture for implementing a smart city governance solution using Blockchain technology.
- To ensure a secure, open, and auditable process for handling citizen requests and services.

- To create smart contracts for automating service delivery and minimizing bureaucracies.
- To come up with a metadata framework for enabling tracking, validating, and auditing of each citizen request.
- To test the performance and latency of the proposed model compared to existing models.

4.1 System Architecture

The suggested system architecture will comprise a modular, scalable, and distributed system that utilizes the concept of blockchain technology. This system will facilitate various types of services like permits approval, grievances redressal, resource booking, and many more using a digital platform. In addition, the proposed system will be a completely decentralized network in which each node will contribute to performing any activity or validating any data regardless of the authority or department managing that node.

This suggested system architecture incorporates the citizen interface, the services app, the trust framework, distributed data storage, and the Internet of Things technology into one smart city framework. The DFDs present the flow of data in general and detailed views between the citizens, the administrators, the service providers, and the system itself. The sequence diagram describes the flow of a request by the citizen in a chronological order.

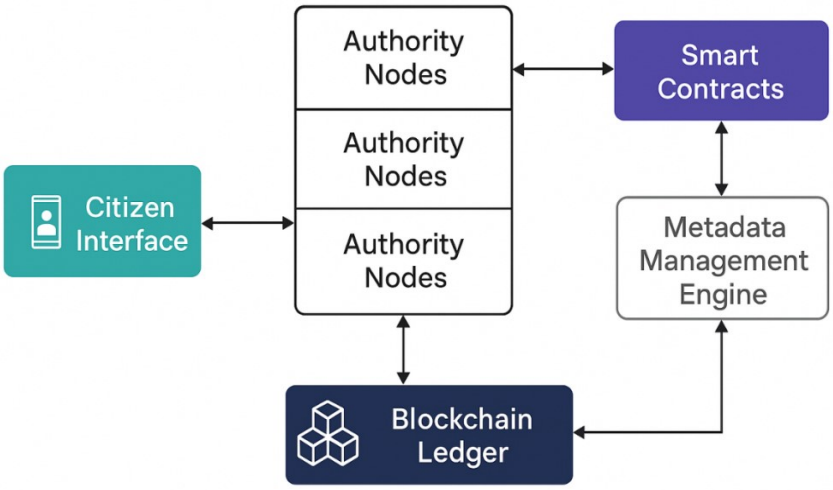


Figure 4.1: Proposed System Architecture

System Participants:

- **Citizens:** End users who make the requests and monitor the status of services using web/mobile applications. Personal identity of citizens is kept anonymous through encryption but they have a hashed user ID in the system.
- **Authority Nodes:** Authority nodes represent the departments or municipalities responsible for verifying citizen requests and signing off on them. Authority nodes are independent but function in consensus with other authority nodes through the blockchain technology.
- **Service Providers:** Service providers refer to the entities who can offer infrastructure/logistical capabilities needed to fulfill citizen requests; may include waste management agencies, electricity service providers, etc.
- **Smart Contracts:** Automated scripts running on blockchain for validating conditions, signing off on processes, and executing certain tasks automatically without human interference.
- **Blockchain Ledger:** Immutable record of all transactions, requests and execution of smart contracts in the blockchain.

4.2 Component Description

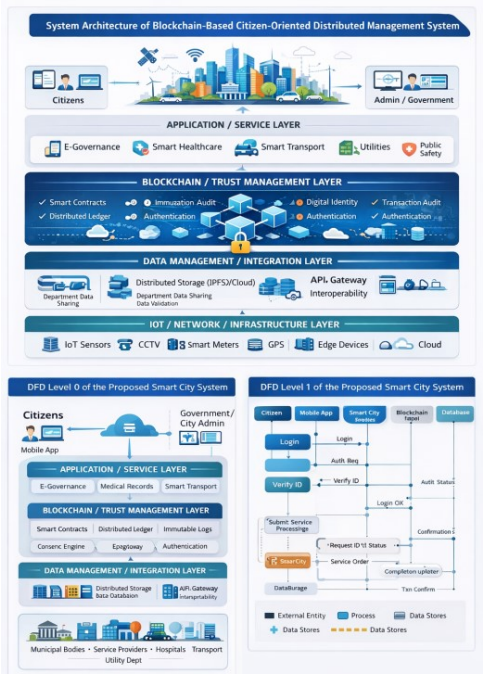


Figure: 4.2. Architecture of Proposed BBCODMS

Citizen Interface (Mobile/Web Application)

The application lets the users log into the system, initiate service requests, update their status, upload files, and give feedback. All transactions have signatures and are encrypted.

Authority Nodes

Each authority node corresponds to an agency or government department that validates citizen's requests within their jurisdiction and interacts with smart contracts and adds new blocks to the chain.

Blockchain Layer

Each citizen request and authority response are registered in blockchain forever. This guarantees that all transactions are immutable.

Smart Contracts

These are self-executing programs containing business logic for various service types. For example, permit approval contract determines whether the applicant meets the requirements and provides necessary documents. Once all conditions are fulfilled, the contract automatically sets request status to "Approved."

Metadata Management Engine

This engine collects transaction data, including ID and timestamp of the transaction, status, department id, etc.

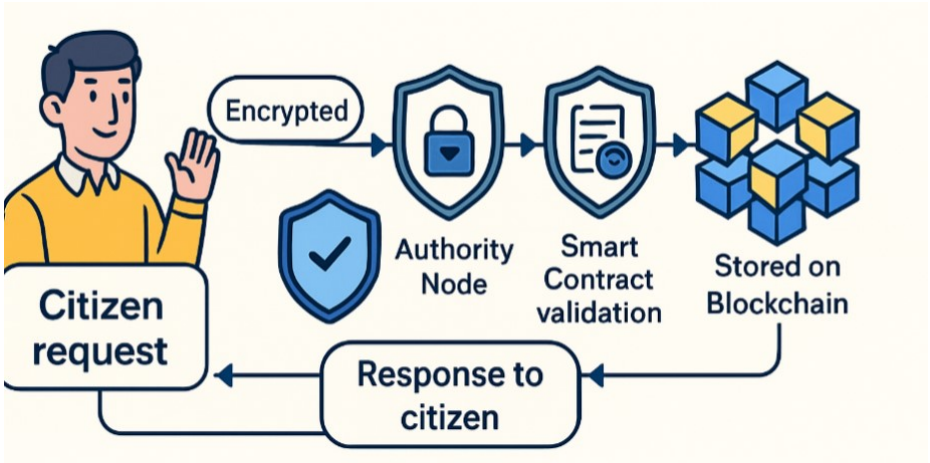


Figure 4.3: Transaction Flow from Citizen to Blockchain via Smart Contract

4.3 Metadata Structure

4.3.1 Metadata Fields

Metadata plays a crucial role in ensuring that each transaction, though anonymized, can be audited, analyzed, and processed meaningfully. The system captures a specific set of metadata fields for each citizen service request.

Table 4.1: Metadata Schema for Citizen Transactions

Field Name	Data Type	Format	Required
citizen_id_hash	String	SHA-256	Yes
request_id	String	UUID	Yes
service_type	String	Enum (e.g., GRV, LIC)	Yes
timestamp	Datetime	ISO 8601	Yes
contract_ref	String	Contract Address	Yes
node_id	String	Alphanumeric	Yes
status	String	Enum (Pending, Approved, Rejected)	Yes
feedback	String	Text (Optional)	No

4.3.2 Smart Contract Logic

Every smart contract entails a specific set of rules regarding service operations. These rules get activated automatically based on the transactions' metadata, user authorizations, or predetermined criteria.

Use Case Examples:

- Permit Application Smart Contract: Determines whether documents have been submitted and if the applicant qualifies for the permit.
- Grievance Redressal Smart Contract: Escalates grievances after a specified time period.
- Resource Scheduling Smart Contract: Ensures resource availability and schedules according to first-come-first-served basis.

Table 4.2: Smart Contract Conditions and Execution Rules

Service Type	Trigger Condition	Smart Contract Action
Permit Approval	All documents uploaded, eligibility verified	Auto-approve, notify citizen
Grievance Redressal	No response in 48 hrs	Escalate to higher authority node
Utility Connection	Payment verified and location matched	Initiate service scheduling
Public Resource Booking	Date/time slot availability	Confirm booking and issue token
License Renewal	Expiry within 30 days, no violation record	Auto-renew and send digital copy

This structure ensures **service automation**, reduces human error, and delivers **fast, transparent, and auditable outcomes** to citizens. The next section will evaluate how this system performs in real-time environments and how it compares to legacy frameworks.

4.4 Blockchain Consensus Mechanisms

A consensus mechanism is an important protocol that helps the network's nodes reach an agreement about the current state of the blockchain ledger. Consensus protocols play an important role in decentralized networks since they help achieve this agreement without a central authority. They determine the speed, scalability, energy consumption, and level of security of a blockchain-based system—issues relevant to its deployment in smart cities [59].

4.4.1 Proof of Work (PoW)

The Proof of Work protocol makes nodes (called miners) solve difficult cryptographic problems to confirm transactions and add new blocks to the blockchain. This protocol offers a high level of security and decentralization; however, it is very resource-demanding and energy-consuming, making it inappropriate for smart city solutions.

Application in Smart Cities: Not suitable because of latency and energy.

Proof of Work (PoW) – Mathematical Model

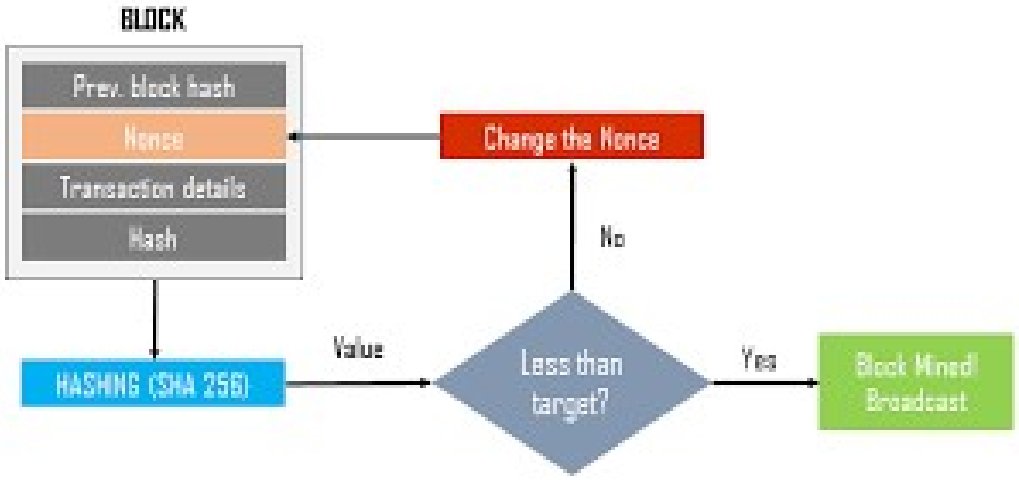


Figure 4.4: Flow Diagram of Mathematical Model

Model Equation

$$H(n \| b) < T$$

Where:

- **H**= Cryptographic hash function (e.g., SHA-256)
- **n**= Nonce
- **b**= Block data
- **T**= Target threshold (difficulty level)

Interpretation

- Miners repeatedly compute hash values until a valid nonce is found.
- Lower **T**⇒ higher difficulty ⇒ more computation required

Proof of Work (PoW) Flowchart



Figure 4.5: Flowchart for Proof of Work (PoW)

Steps

1. Collect transactions

2. Create block

3. Initialize nonce

4. Compute hash

5. Check: **Hash** $< \boldsymbol{Target}$?

- Yes → Broadcast block
- No → Increment nonce and repeat

4.4.2 Proof of Stake (PoS)

In Proof of Stake, validators are chosen based on the number of tokens they stake in the network. It requires less energy, offers faster validation, and encourages good behavior as dishonest actions can lead to loss of staked assets.

Use in Smart Cities: More feasible than PoW. PoS-based systems can support real-time applications such as smart traffic lights or utility billing systems.

Proof of Stake (PoS) – Mathematical Model

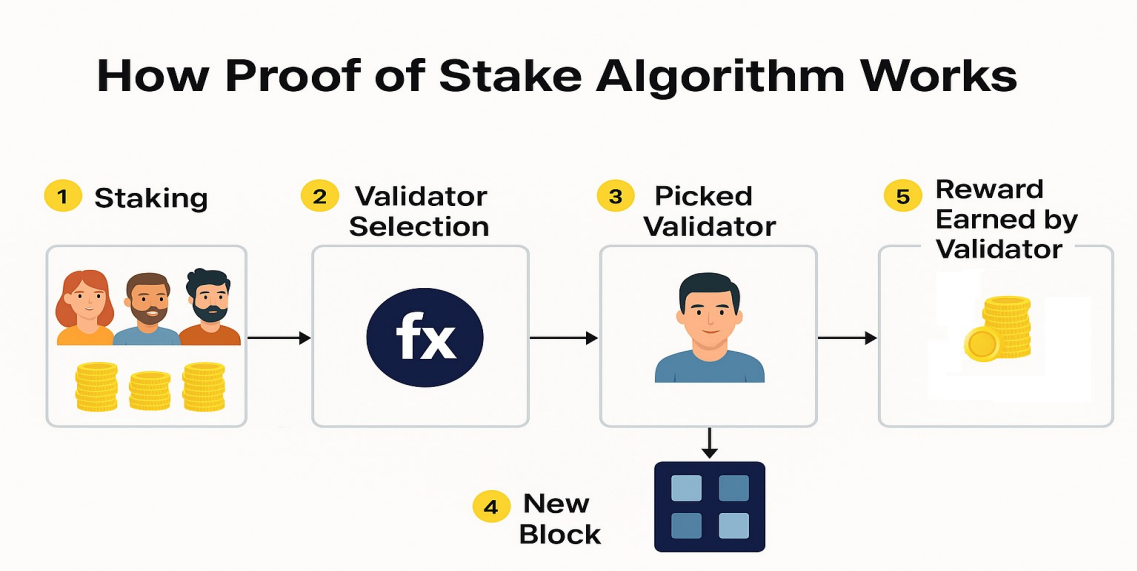


Figure 4.6: Flow Diagram of Mathematical Model for PoS

Validator Selection Probability

$$P_i = \frac{S_i}{\sum_{j=1}^{N} S_j}$$

Where:

- P_i= Probability of node **i**being selected
- S_i= Stake of node **i**
- **N**= Total validators

Interpretation

- Higher stake ⇒ higher probability of being selected.
- Energy-efficient compared to PoW.

Proof of Stake (PoS) Flowchart

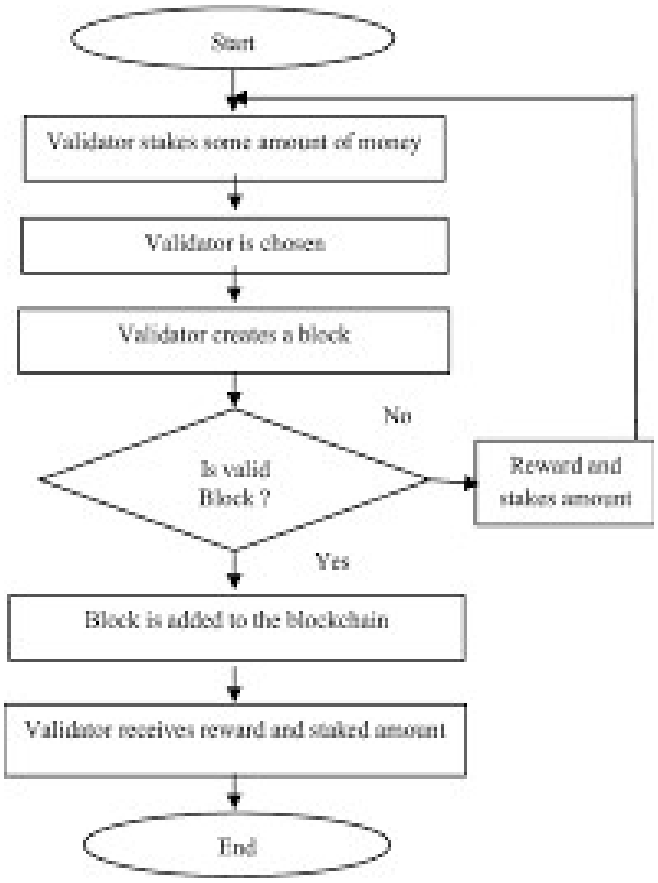


Figure 4.7: Flowchart for Proof of Work (PoW)

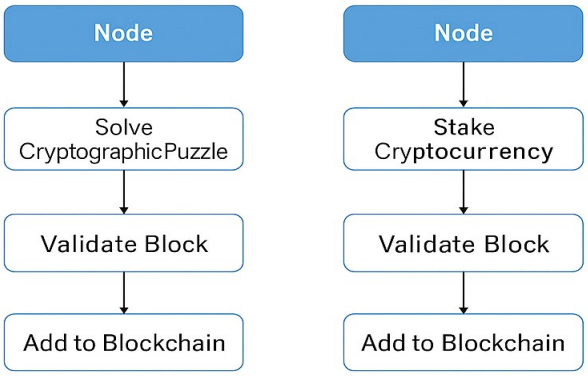


Figure 4.8: Visual Representation of PoW vs PoS

A flow diagram comparing PoW and PoS: from node selection to block validation, highlighting resource requirements and speed.

Steps

1. Validators stake tokens
2. System selects validator (based on stake/randomness)

3. Selected validator proposes block

4. Other validators verify

5. Block added to chain

6. Rewards/Penalties applied

4.4.3 Delegated Proof of Stake (DPoS)

DPoS can be seen as a development of PoS, whereby delegates (validators) are elected by stakeholders to create blocks in their stead. It greatly enhances scalability and transaction speeds, yet it does have the potential to lessen decentralization.

Use in Smart Cities: Ideal for implementation within smart cities that require quick consensus to be reached, with accountability built into their system (e.g., government departments).

4.4.4 Practical Byzantine Fault Tolerance (PBFT)

PBFT is designed for permissioned environments. It allows nodes to reach consensus despite a few nodes acting maliciously, provided two-thirds act honestly. PBFT ensures low latency and high throughput and doesn't require high computational power.

Use in Smart Cities: Ideal for private or consortium blockchain deployments, such as citizen identity management, land registries, and e-governance services.

PBFT (Practical Byzantine Fault Tolerance) – Mathematical Model

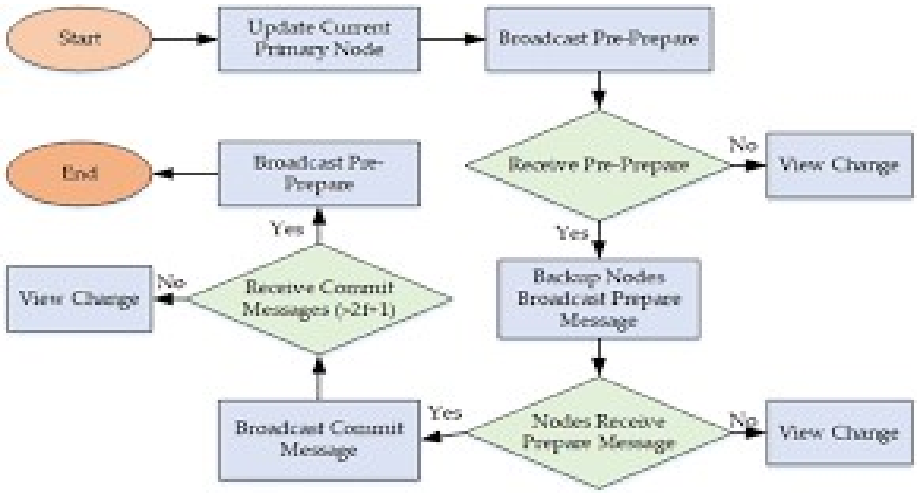


Figure 4.9: Mathematical Model for PBFT

Fault Tolerance Condition

$$\mathbf{n \geq 3f + 1}$$

Where:

- **n**= Total nodes
- **f**= Maximum faulty nodes tolerated

Consensus Condition

Valid if $\geq \mathbf{2f + 1}$ nodes agree

Interpretation

- System tolerates up to **f**malicious nodes.
- Requires supermajority agreement.

Steps

1. Client sends request

2. Primary node → Pre-prepare phase

3. Nodes → Prepare phase (broadcast)

4. Nodes → Commit phase

5. If $\geq 2f + 1$agreement → Execute request

6. Reply sent to client

A number of consensus algorithms have been deployed in the architecture in order to ensure security, scalability, and efficiency. The proof of work algorithm provides security because of the complexity of computation, while the proof of stake algorithm provides higher energy efficiency due to validation based on stakes. Lastly, the PBFT algorithm ensures quick consensus in fault tolerant permissioned networks.

Table 4.3: Comparative Analysis of Consensus Mechanisms

Feature	PoW	PoS	DPoS	PBFT
Energy Usage	Very High	Low	Low	Very Low
Transaction Speed	Slow	Moderate	Fast	Very Fast
Scalability	Low	Moderate	High	High
Fault Tolerance	High	Moderate	Moderate	High
Decentralization	Very High	High	Medium	Low
Suitability for Smart City	Low	Medium	High	Very High

4.4.5 Consensus Mechanisms in Smart City Infrastructure

With respect to smart cities, the consensus algorithms have to be compatible with the following:

- Low latency for making decisions on time (for example, in emergency systems).
- High transaction throughput, capable of processing thousands of transactions per day.
- Energy efficiency, as sustainability is one of the pillars of smart cities.
- Traceability and accountability, especially for governance-based services.

Whereas public blockchain networks such as Bitcoin and Ethereum use Proof of Work (PoW) and Proof of Stake (PoS), both of these models are less likely to be relevant to smart city use cases, considering performance and ecological aspects. Practical alternatives include Proof of Authority (PBFT) and Delegated Proof of Stake (DPoS), which are better suited to the consortium permissioned blockchain model that smart cities will employ.

4.5 Core Components of Smart Cities

Smart cities can be understood as complex and highly interconnected ecosystems that use digital technology within the physical environment and socio-cultural landscape of an urban area. The essential features of a smart city focus on effective governance of the city, proper management of resources, intelligent transportation, sophisticated healthcare, and efficient utility services. It is essential for all of these aspects to work

together in order to provide an improved standard of living and ensure optimal use of resources.

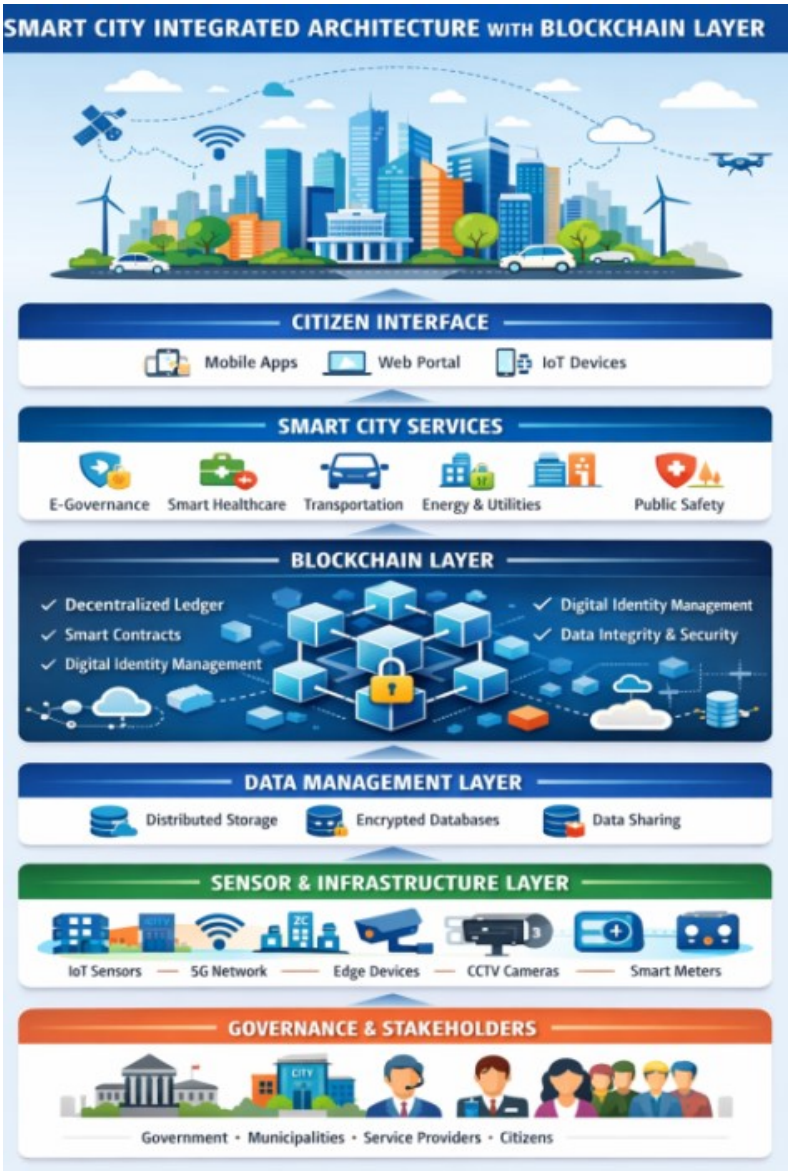


Figure 4.11: Smart City Integrated Architecture

4.5.1 Smart Governance

Smart governance forms the base of any smart city. Smart governance refers to the use of technology-enabled platforms in order to improve responsiveness, accountability, and transparency in the delivery of government services. The basic idea behind smart governance is to shift away from traditional administrative processes towards participative and data-oriented governance processes.

The basic features of smart governance include the following:

- **E-Governance:** All public services will be provided electronically via the portals of central citizens, thus reducing physical interface in the process and ensuring round-the-clock availability of services such as registration of births, payments for utility bills, complaints submission, and document validation.

- **Participatory Governance:** Citizens are considered stakeholders in the governance process as against beneficiaries. Participation of citizens in the decision-making process is ensured through mechanisms such as online voting, opinion polls, and other participative citizens' platforms.

- **Real-Time Decision Making:** Authorities are able to constantly monitor and evaluate the performance and functioning of cities by making real-time analysis and using data received from IoT sensors, geographic information system (GIS), and engagement of the public via online channels.

- **Digital Identity:** Identification and authentication of citizens using digital identity technology similar to Aadhar biometrics helps improve citizen inclusion in accessing public services.

4.5.2 Smart Energy

The main purpose of the smart energy system is to provide effective, secure, and sustainable energy generation, transmission, and consumption in an urban setting. In smart cities, the energy supply is developed in a way that allows the system to respond in real-time to changing consumption rates while limiting its reliance on fossil fuels.

Components of smart energy systems:

- **Smart Grids:** They are digitalized electrical grids that offer bidirectional communication between the utility and consumers. Smart grids can track electricity usage, recognize outages, equalize loads, and accommodate alternative power generators such as home solar installations.

- **Integration of Renewable Power Generation:** The goal in smart cities is to incorporate the use of alternative energy technologies such as wind, solar, and waste-to-energy. Through advanced prediction and grid-tied inverter technology, renewables are easily accommodated within current power supplies.

- **Real-time Pricing and Demand Management:** Off-peak power consumption is encouraged through dynamic pricing tariffs which help to manage demand.

- **Real-time monitoring of Energy Consumption**: With smart metering systems installed in both houses and office buildings, energy usage is tracked and monitored in real-time allowing for informed decisions to be made about supply.

Smart energy systems decrease energy wastage and expenses while ensuring sustainability and resiliency of urban infrastructure.

4.5.3 Smart Health

Smart city health systems depend on three important elements—connectivity, interoperability, and intelligence of data—to ensure more efficient, more accurate, and more balanced delivery of healthcare services. Smart health is associated with the preventive approach, remote access to healthcare services, and personalized approach enabled by technology.

The primary elements of smart health involve:

- **Telemedicine and remote diagnostics:** Citizens may seek medical help from doctors using video communications; this type of solution becomes even more efficient when used in distant locations. Integration with AI technologies allows for an even greater precision in remote diagnosis.

- **Management of health-related data:** Electronic health record (EHR) systems provide centralized access to the medical history of patients, allowing for a consistent provision of medical care. The use of blockchain technologies may ensure greater security of the information.

- **Emergency response systems**: Smart ambulances provided with GPS trackers and telemedicine equipment are sent according to real-time data about the road condition and accidents. This way, integration of the system allows for better coordination of actions in case of emergencies.

- **Wearable devices and IoT-enabled health sensors:** Smart watches and similar biometric devices track the health metrics such as pulse rate, glucose level, and oxygen saturation of blood.

4.5.4 Smart Mobility and Transport

One of the features of smart city is its effective urban mobility. Smart mobility refers to an integrated system for transportation that aims to optimize efficiency, reduce pollution, reduce travel time, and maximize access and convenience for travelers.

Key elements include:

- **Intelligent Transport Systems (ITS):** The system uses traffic sensors, GPS technology, predictive analysis through artificial intelligence, and signal control to manage congestion. Updates on real-time traffic conditions aid in navigation and emergency response routing.
- **Public Transport Optimization:** Through the use of data analysis, route optimization is possible. There are real-time passenger information systems as well as apps that allow commuters to monitor bus train schedules and routes, delays etc.
- **EVs and Autonomous Driving:** Many smart cities plan on including electric vehicles and autonomous driving technologies to be more innovative and sustainable.
- **Multimodal Integrated Fare System:** Integrated smart fare system that allows travel between buses, metro trains, ferries, bicycle sharing stations, and other transport options.
- **Demand Management:** Smart parking through use of Internet of Things technologies ensures that the driver is directed towards a free parking space minimizing unnecessary car movement.

These advancements result in decreased traffic congestion, pollution, and increased accessibility among all demographics.

4.5.5 Smart Waste and Water Management

Utility management, especially waste and water management, is essential for sustainability and good health in the city. Intelligent management systems for waste and water will conserve resources, improve reaction times, and increase operational efficiency.

The most important initiatives are as follows:

- **The IoT Enabled Waste Bins:** These smart waste bins have level sensors which can alert municipal agencies when their bins become full. The system helps optimize truck routes and save on fuel while keeping hygiene standards high.
- **The Recycling Monitoring and Waste Segregation Initiative:** By implementing intelligent bin labels along with artificial intelligence-based image recognition, it will be easier to recycle waste.
- **Water Usage Management:** Digital water meters will enable real-time measurement of water consumption, and underground pipeline leaks will be detected using pressure sensors.
- **Smart Irrigation System:** Soil moisture sensors will enable automation of park irrigation systems.
- **Stormwater and Sewerage Systems Monitoring:** This will enable detection of flooding, sewage flow levels, and avoid overflows into urban areas.

4.6 Citizen-Centric Design Principles

As smart cities grow and progress with their technological advancements and connectivity, it is vital for them to retain their foundation on citizen-oriented values. The performance of the smart city cannot be measured only in terms of the use of advanced technology; instead, it needs to be measured in terms of how much power, improved quality of life, and access to public facilities have been provided to individuals. Below are listed some of the fundamental principles of citizen-oriented design. The following figure shows Eco-system for Citizen-Oriented Smart City.

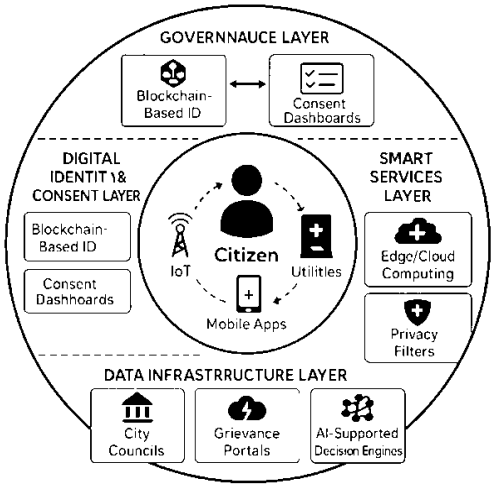


Figure 4.12: Citizen-Oriented Smart City Ecosystem

4.6.1 User-Centered Design in Urban Planning

The bedrock of a smart city geared towards its citizens depends on user-centered design (UCD). When it comes to urban design, UCD simply means an iterative process by which the requirements, behaviors, preferences, and desires of the inhabitants of the city are made central to all decisions and designs related to city construction. Traditional infrastructure development for urbanization has always been based on the top-down approach, however, a contemporary smart city requires a bottom-up approach, wherein the citizens themselves co-develop solutions along with the other experts.

It includes:

- Engaging the citizens via online forums, public meetings, surveys, and feedback loops.
- Collecting data using mobiles, sensors, and social media to understand the behaviour of the people and plan accordingly.
- Developing an environment that responds to the inputs provided by the citizens in real time.
- To make sure we have human-sized cities that make efficient use of space while ensuring safety and convenience.

4.6.2 Digital Identity, Data Privacy, and Consent

In the context of a smart city environment wherein all services run digitally, it becomes essential to establish a system of secure digital identity. The interaction between citizens and the various services offered either by government agencies or private firms takes place on digital platforms – whether it pertains to paying utilities, accessing health care, or engaging with e-governance systems. Digital identity needs to be:

- Verifiable
- Interoperable
- Privacy-preserving

Technologies like blockchain-based digital identities, zero-knowledge proofs, and decentralized identifiers (DIDs) are some recent developments which ensure self-sovereign identity (SSI). This means citizens retain ownership of their personal data.

At the same time, privacy and consent management become an equally important factor. Smart cities collect a lot of data using devices like CCTV cameras, IoT sensors, smart meters, or even from mobile applications. If no regulation governs this process, there will be chances of surveillance or other unethical practices. Hence, smart cities need to incorporate:

- Explicit methods of collecting consent for data collection/usage.
- Methods of anonymizing data and encrypting it.
- Data governance policy indicating ownership of the data, access permissions, and intended use.

These aspects are ensured if a city complies with regulatory bodies like GDPR.

4.6.3 Service Personalization and Accessibility

Personalization has been identified as one of the most important benefits of a smart city. For instance:

- Personalized public transport applications that suggest travel routes according to the past user data and current traffic information.
- Healthcare systems that personalize preventive healthcare advice according to the health data of the users.
- Smart waste management programs that function according to fill-level sensor data.

The above personalized services would only work effectively when there is an integrated digital platform with sophisticated backend algorithms and artificial intelligence systems. But this personalization must not hinder the inclusiveness of the process. This can be achieved if:

- The services are designed in multiple languages so that people from different backgrounds can use them.

- The design incorporates voice command facilities along with other assistive techniques for differently-abled citizens.
- The program should have an offline version for those areas where Internet connectivity is lacking.

4.6.4 Inclusion of Marginalized Populations

Inclusivity does not only mean providing marginalized people access to technology but also involving them in policy-making processes, decision-making bodies, and allocation of resources. The marginalized groups include poor urban dwellers, women, elderly persons, ethnic minorities, migrants, and people with disabilities. Citizen-oriented planning will include:

- Participatory budgeting and digital platforms for filing grievances especially targeting disadvantaged individuals.
- Subsidies and digital coupons for necessary services like electricity and healthcare.
- Use of mobile apps for helping migrant labor access legal assistance, education, and employment opportunities.
- Gender-appropriate infrastructure including well-lit areas and safe modes of public transport.

Blockchain can help ensure that there are tamper-proof records for beneficiaries. On the other hand, machine learning algorithms can identify and eliminate algorithmic biases.

4.7 Smart City Reference Architectures

The creation and successful application of smart cities depend on effective architectural frameworks, which serve as a standardized blueprint for incorporating technical, organizational, and governance elements into smart cities. Such frameworks enable alignment between the interests of multiple parties involved in creating smart cities including government entities, service providers, residents, and technology vendors, thus providing a roadmap for the implementation of smart services in different areas like energy, transportation, governance, environment, and healthcare.

During the last ten years, several organizations, both international and local, have been proposing reference architectures for smart cities. In order to cope with the ever-

growing complexity of urban areas and facilitate interoperability, security, scalability, and citizen-centricity, a number of reference models have been offered. The following paragraphs describe three important reference models – ITU-T Y.4208, ISO 37106:2018, and SACFA (Smart City Architecture Framework) introduced in India.

4.7.1 ITU-T Y.4208 Reference Architecture

Recommendation Y.4208 by the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) provides an architectural framework for the sharing and management of smart city data. This architecture mainly addresses issues of interoperability and security of information exchanges within cities.

Core elements of recommendation Y.4208 are as follows:

- **Sensing Layer:** It consists of data acquisition mechanisms that include IoT devices, environmental sensors, surveillance cameras, and citizen contributions.
- **Data Exchange Layer:** Involved in normalizing, cleansing, fusing, and transferring data securely from one platform to another.
- **Data Management Layer:** It takes care of storing, processing, analyzing, managing metadata and access control over data.
- **Application Layer:** Delivers end-user applications that encompass dashboard portals, mobile apps, and decision-making using Artificial Intelligence.
- **Governance Layer:** Defines policy issues related to data usage, ownership, liability, and compliance.

Recommendation Y.4208 highlights the importance of semantic interoperability among various systems. Recommendation Y.4208 favors the open API architecture.

4.7.2 ISO 37106:2018 Smart City Operating Model

The ISO 37106:2018 standard created by the International Organization for Standardization (ISO) sets out a comprehensive governance approach to support the creation of smart cities. Unlike other standards that prescribe technology, ISO 37106 sets out the approaches and operating principles a city must follow to ensure sustainability, resiliency, innovation, and citizen participation.

Important components of the ISO 37106 standard include:

- Operating principles: Openness, flexibility, scalability, citizen-centricity, and continuous improvement.
- Digital transformation enablers: Favors ICTs like cloud computing, big data analysis, Internet-of-Things (IoT), and blockchain technologies.
- Governance models: Emphasizes cross-sector cooperation, citizen involvement, and horizontal integration across city departments.
- Performance management: Measures progress against outcome-oriented KPIs to determine the effectiveness of a smart city in enhancing quality of life, economic prosperity, and sustainability.

The ISO 37106 standard is perfect for strategic planning and policy development. It is commonly used in conjunction with architectural frameworks to ensure that the deployment of technology is aligned with overall city objectives.

4.7.3 India's Smart Cities Reference Architecture (SACFA)

In India, MoHUA has introduced SACFA (Smart Cities Application Framework Architecture) in the context of the Smart Cities Mission. SACFA intends to design a standardized, scalable, and interoperable framework to help over 100 smart cities.

SACFA is built on the foundation of five layers:

- The Device and Network Layer consists of all the field devices such as CCTVs, environmental sensors, RFID readers, traffic counters, and network connectivity such as fiber, Wi-Fi, 4G/5G.
- The Data Acquisition Layer involves collecting and converting real-time data into structured data form.
- The Data & Platform Layer comprises data lakes, analytics engines, blockchain-based registries, and identity management solutions.
- The Application Layer supports applications such as Smart Traffic Management, Solid Waste Monitoring, Smart Water Metering, and Integrated Command and Control Centers (ICCC).

- The Governance & Integration Layer covers compliance requirements, data privacy, open APIs, service-level monitoring, and third-party integrations.

SACFA follows the concept of the Open Digital Ecosystem (ODE), which facilitates citizens' participation and vendor neutrality while designing an ecosystem of solutions for innovation. In line with India's efforts towards digital transformation, India.

4.7.4 Common Layered Architecture in Smart Cities

Despite their differences, most smart city reference architectures share a common layered model that separates concerns and enhances modularity, scalability, and integration across services. The standard five-layer model is described below:

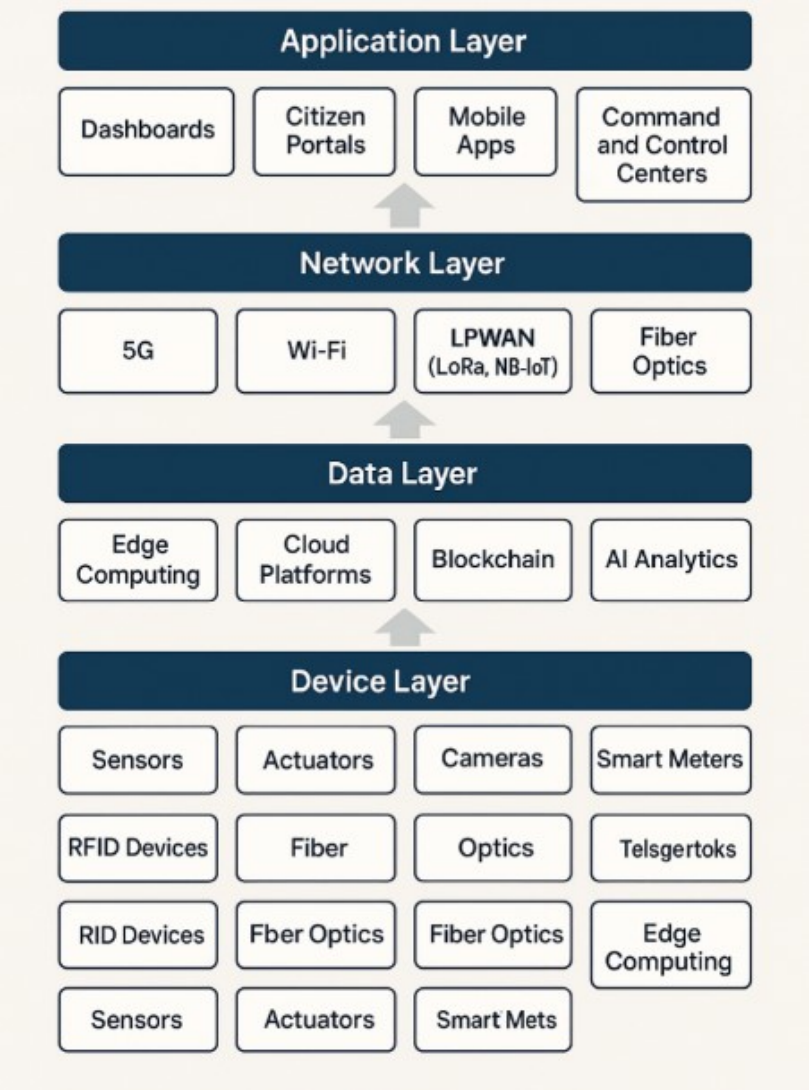


Figure 4.13: Smart City Layered Architecture

Table 4.4: Layer Description

Layer	Description
Sensing Layer	Physical layer consisting of sensors, IoT devices, and citizen data input tools.
Network Layer	Communication infrastructure: wireless, wired, and mesh networks.
Data Layer	Cloud and edge platforms for data ingestion, storage, analytics, and security.
Application Layer	Smart services (e.g., mobility, waste, e-governance) accessed via APIs and apps.
Governance Layer	Oversight for policy enforcement, compliance, service orchestration, and ethics.

This layered approach ensures that cities can evolve over time by upgrading one layer (e.g., application) without disrupting others (e.g., data or sensing). It also supports interoperability, data standardization, and resilience to technological change.

4.7.5 Comparative Analysis of Reference Models

Table 4.4: Comparison of Global Smart City Reference Frameworks

Framework	Focus Area	Orientation	Layers Included	Citizen-Centric?	Interoperability Support
ITU-T Y.4208	Data Architecture	Technical	Yes (5-layered)	Moderate	High
ISO 37106:2018	Governance	Strategic/Policy	No (focuses on principles)	High	Moderate
SACFA (India)	Nationwide Deployment	Technical + Operational	Yes (5-layered + ICCC)	High	High

Smart city reference architectures constitute the framework that is needed to build an integrated smart city. These architectures constitute the support on which various technical components, as well as governance and citizen services, will be developed. While the ITU-T Y.4208 reference architecture is highly effective when it comes to data interoperability, ISO 37106 provides a valuable strategy in terms of inclusive governance, and SACFA offers an effective framework that is designed to scale for a national roll-out.

CHAPTER-5

Results & Analysis

Results & Analysis

Performance Evaluation Setup

It was required to design a real-time simulation environment that would be based on the mentioned-above blockchain citizen-centric distributed management system and that would leverage the newest blockchain technologies and solutions.

For implementation purposes, as the base for blockchain architecture, the Ethereum Testnet (Rinkeby) has been selected, and its copy created via Ganache to be able to work on it and develop tests. Also, a ledger based on smart contracts performing citizens' services was designed, while the Truffle development framework was used to code smart contracts. Also, for simulation purposes, to be able to demonstrate citizens' wallets as well as transaction handling, Metamask technology was employed, while for blockchain network deployment and execution log analysis, Go Ethereum (Geth) platform was leveraged.

The designed simulation environment consisted of

- **10 blockchain nodes** distributed across virtual containers (Docker).
- **500 simulated citizen users** generating service requests concurrently (e.g., utility connection, complaint registration, permit requests).
- **4 categories of citizen services**, with differing smart contract execution times and confirmation requirements.

The traditional system benchmark was modeled using a standard relational database (PostgreSQL) backend connected to a centralized web server to mirror legacy e-governance platforms. Both environments were stress-tested under similar load profiles to ensure fairness in comparison.

4.1 System Performance Analysis

For assessing the performance, three crucial factors were taken into account, including throughput, latency, and trust score.

Throughput (Transactions per Second – TPS)

The term “throughput” stands for the ability of the system to manage several transactions at the same time. According to the performance analysis, in the case of blockchain implementation, the system could process 450 TPS during the continuous functioning under 500 users; meanwhile, the traditional solution could provide a maximum of 120 TPS.

Such an excellent improvement in the throughput rate can be explained through the blockchain-based system’s distributed transaction management and automation with the help of smart contracts. The service approval was done automatically through smart contracts without sending any information back to central parties.

Latency

Latency, described as the period between the submission of the request and confirmation/response, was important for citizen experience. On the blockchain platform, transaction confirmation latency took on average 0.8 seconds while that in the traditional platform it took 2.3 seconds. Latency was caused by queuing at processing nodes and manually verifying the transactions in the traditional platform. This was because blockchain transactions were verified through consensus without any need for administrative confirmation; hence, the response time improved by 65.2%.

Trust Score

The trust score was calculated based on simulated responses by the citizens and system metrics. The citizens were shown post-service surveys to indicate how confident they were of the system's fairness, transparency, and promptness. The blockchain platform received an average score of 91.3/100 while the traditional platform had 68.5/100, indicating a 33.3% improvement in response time.

Graphical Results

The performance improvements are visually summarized in the following figures

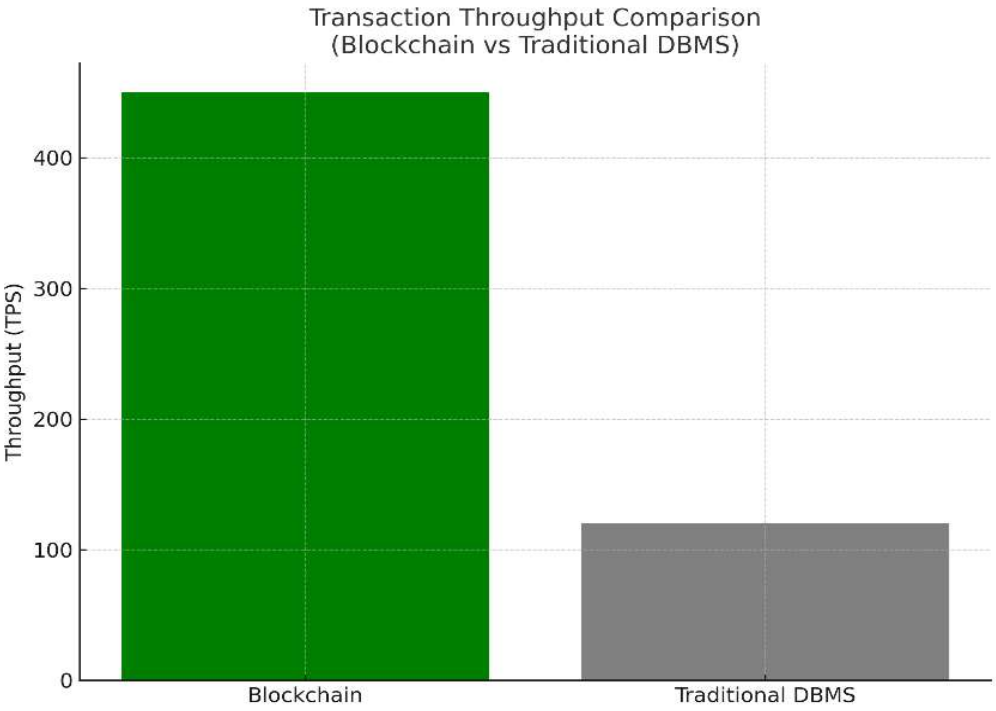


Figure 5.1: **Transaction Throughput Comparison (Blockchain vs. Traditional DBMS)**

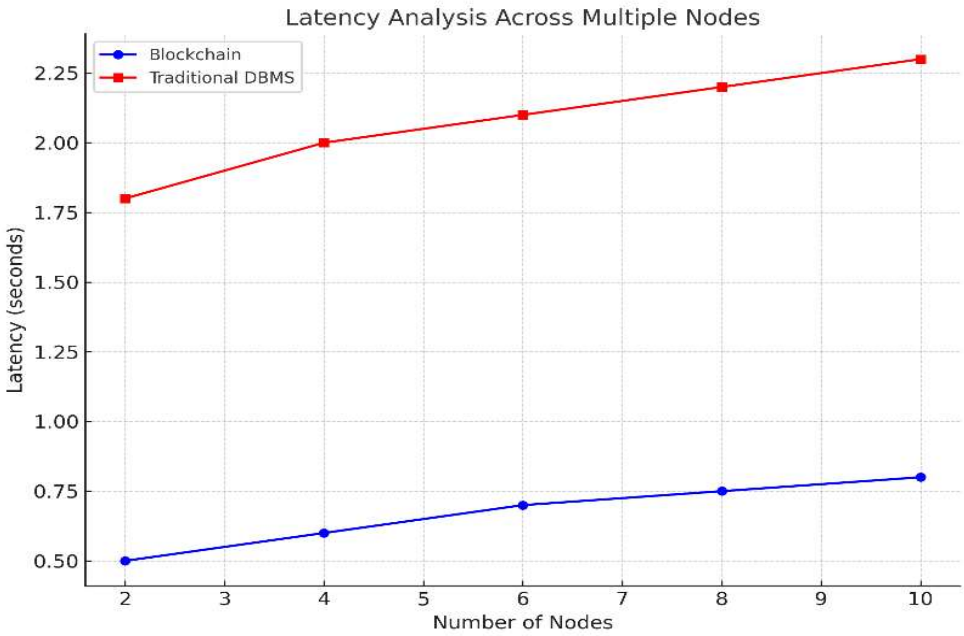


Figure 5.2 : **Latency Analysis Across Multiple Nodes**

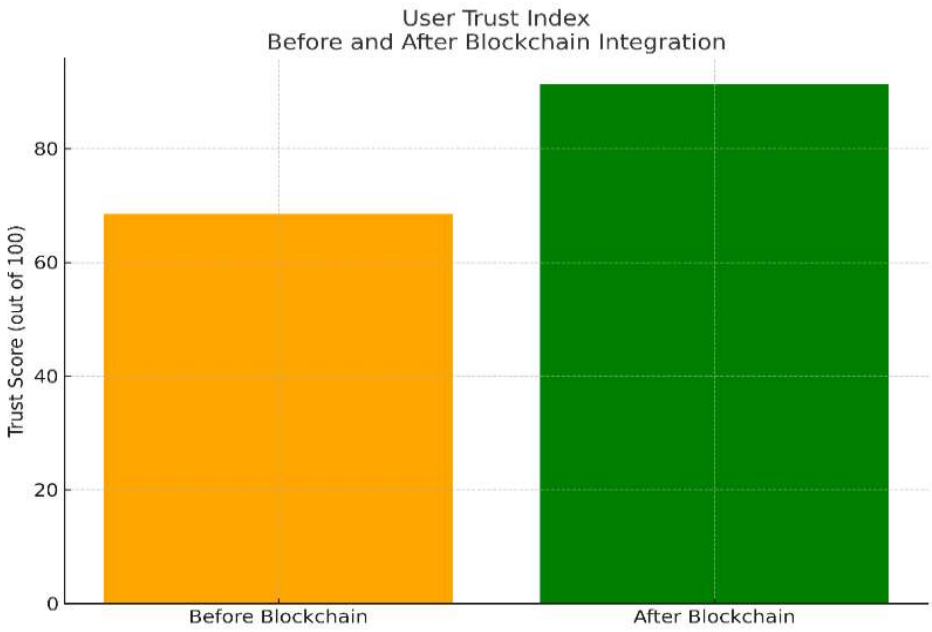


Figure 5.3: **User Trust Index Before and After Blockchain Integration**

These graphs clearly depict the scalability and responsiveness of the blockchain framework compared to its legacy counterpart.

Table 5.1: Performance Metrics Summary

Metric	**Blockchain System**	**Traditional System**	**% Improvement**
Throughput	450 TPS	120 TPS	275%
Latency	0.8 sec	2.3 sec	65.2%
Trust Score	91.3 / 100	68.5 / 100	33.3%

5.2 Security and Privacy Analysis

Security and privacy are essential for citizen service management in smart cities. The blockchain-based solution was compared to the existing one in terms of the following parameters: data integrity, immutability, robustness of access control measures, privacy/anonymity, and auditability.

Immutability and Auditability

Since blockchain technology guarantees immutability of the data recorded on the network, this feature allows avoiding any modifications after a certain event takes

place, which can be easily done in a standard database management environment. Each transaction can be traced and validated, making system audit possible.

Access Control and Encryption

Role-Based Access Control (RBAC) was deployed in smart contracts that allowed performing write operations only to authorized nodes (municipal departments, service providers). Perimeter security is often employed in the traditional setup, but in case of breaching perimeter boundaries, the whole database becomes accessible to malicious users. Besides, data were encrypted with elliptic curve cryptography (ECC) before being added to blockchain.

Resistance to Attacks

The new model is highly resistant to typical attacks like:

- Spoofing, protected by the use of asymmetric cryptography based on public-private keys.
- Denial of Service (DoS), which is addressed by decentralization and load balancing.
- Replay attacks by verifying nonces and timestamps.

Table 5.2: Security and Privacy Score Evaluation

Parameter	Score (Blockchain)	Score (Traditional)
Data Integrity	10 / 10	6 / 10
Tamper Resistance	10 / 10	5 / 10
Access Control Strength	9 / 10	7 / 10
Anonymity / Pseudonymity	8 / 10	3 / 10
Auditability	10 / 10	6 / 10

The results clearly reflect that blockchain-based systems offer superior safeguards for citizen data while complying with legal and ethical standards for transparency and privacy.

5.3 Comparative Analysis with Conventional Systems

Some of the key operational advantages of using a blockchain-based citizen management system include:

- Discarding the Process Bottlenecks Associated with Manual Processes: Automated smart contracts ensure that service requests from the citizens are processed effectively without any delays. In the traditional systems, all processes were done manually, and therefore, delays could occur.
- Fast Decision Making Mechanism: The contract rules allow authorities to make timely decisions on standard requests put forth by citizens, such as provision of water connections to households. Decisions made using traditional systems could take quite some time.
- Monitoring Performance: Any feedback provided by the citizens through the system is immutable and can be traced back to a certain transaction. It can be used to assess the performances of individual departments or nodes in the system.
- Timesaving Measures for the Authorities: With respect to validating requests, resolving disputes, and audits being automated, the system allows the authorities to devote their efforts into policy development instead.
- Reduced Number of Disputes Due to Immutability of Data: Transactions in the system are immutables because of the time-stamping mechanism. As a result, there will not be many cases involving manipulation of records or disputes.

CHAPTER-6

Discussion

Leveraging Blockchain Technology within Smart City Implementations

6.1 The Multifaceted Impact of Blockchain Technology on Smart Cities

However, the emergence of blockchain technology has been groundbreaking for digital systems currently in use, especially for creating intelligent cities. An intelligent city is defined as one where the use of ICTs is utilized to enhance the efficiency of operations and make people enjoy a better experience living in such cities. Traditional ICT systems have been criticized for having centralized, transparent, and ineffective means of data handling. Blockchain technology, on the other hand, forms the backbone for efficient digital identification, real estate management, utilities management, governance, and transportation in a smart city.

Blockchain enhances efficient digital identification in a smart city. Individuals normally carry many IDs issued by different departments of the government, which leads to redundancy and even possible fraud cases. Blockchain technology enables individuals to develop a digital ID, which is stored on a decentralized ledger. This is an encrypted identification process that is universally accepted among all municipal service providers. In this case, service delivery becomes more efficient, eliminates any fraudulent processes, and increases individual control of personal information.

Property/land registration represents another industry sector in which changes have been significant. Old techniques for recording land titles and ownership records can easily be compromised as they may involve corruption, inefficiencies, and manipulation of data entries. Blockchain technology ensures that titles, data on ownership, as well as the recording process for land transactions and disputes are immutable. What it means is that an individual trying to manipulate land titles will be required to seek approval from all other nodes. Lastly, blockchain technology can prove effective when managing municipal public utility services such as electric power supply and water supply services. Problems associated with inefficiency of billing schemes, tracking of consumption levels, as well as mismanagement of resources become quite evident in

the provision of these services. Combining blockchain technology with the utilization of smart meters, one is able to implement an automatic billing system based on actual consumption. Consumers will have the ability to access their billing history, while the municipality will be able to track the supply and demand trends for better resource allocation. Also, through the use of smart contracts, it becomes possible to implement automatic billing policies where a consumer gets his service disconnected when he exceeds.

In relation to governance, there are many ways through which the use of e-Governance and e-Voting systems can be improved using the security offered by the blockchain technology. Current voting systems are prone to being rigged, manipulated, and lacking transparency. Using blockchain for e-voting makes sure that every single vote is encrypted and uniquely coded to guarantee authenticity, and all votes are stored in a decentralized ledger. Such an approach helps not only ensure higher levels of trust but also increases voter turnout through remote voting capabilities.

Another interesting example of how blockchain technology can improve urban transportation and logistics management is dynamic tolling and pricing using smart contracts. As modern cities experience growing levels of traffic congestion, pollution, and inefficiencies within the public transportation system, the use of smart contracts can automatically adjust pricing to minimize congestion and maximize efficiency. Blockchain also enables secure logging of vehicle movement and maintenance records in a decentralized fashion.

In combination, these examples highlight the effects of blockchain technology in boosting transparency, accountability, and trust within the smart city framework. The elimination of intermediaries leads to the breakdown of information silos, thus facilitating cooperation between various departments. Moreover, immutable records increase the trust citizens have in the impartiality and correctness of the processes carried out in a municipality. Digital citizenship is promoted through transparency and secure participation in governance.

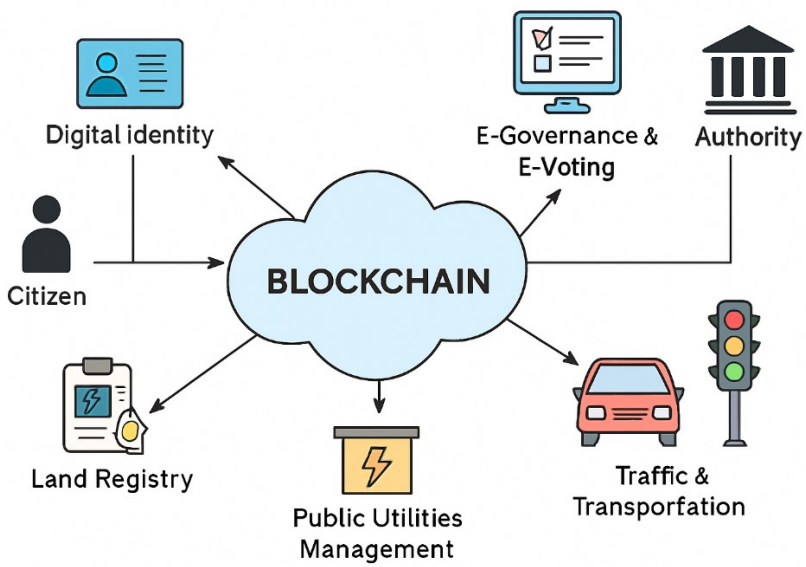


Figure 6.1: Blockchain Use Cases in Smart City Domains

This diagram illustrates blockchain's application across sectors such as identity management, property registration, utility billing, traffic control, and e-voting. It shows interaction flows between key stakeholders—citizens, government authorities, and decentralized blockchain infrastructure—along with data verification checkpoints.

6.2 Blockchain's Role in Enhancing Smart City Security

However, the digital transformation of the urban environment has led to a surge in the use of Internet of Things (IoT) devices within smart cities in the form of interconnected streetlights, surveillance cameras, environmental monitors, traffic management systems, and others. While they improve the efficiency of operations in smart cities, these devices pose substantial cybersecurity risks in the form of potential data breaches, Denial of Service (DoS), unauthorized access, among others. However, the implementation of blockchain technology offers protection against some of the risks posed.

Another important factor is data privacy. Conventional approaches store important data such as citizen files, transaction history, surveillance footage among other data points on central servers that can be easily hacked. A security breach can lead to the entire database being compromised. Decentralized management of data provided by blockchain significantly lowers this risk. In blockchain networks, there is decentralized

control over the network and no single user has the ability to unilaterally change anything. Any attempt to do so requires multiple parties to agree on changing the data.

One more advantage is that blockchains have an audit trail capability. Every entry or transaction that happens within a blockchain ledger is time stamped, tamper-proof, and verifiable. The use of the audit trail capability in smart cities is crucial when there is need for real-time decision-making and the decisions have to be supported by the information recorded. For example, in case a smart utility system does not give a client the expected rebates, a blockchain audit trail will reveal the series of activities that led to the decision made.

Access management is one of the core elements of securing smart cities. Role-based access controls have proved ineffective in preventing cases of privileges abuse and insider attacks. Smart contracts are used in blockchains to implement rule-based access permissions. Smart contracts can automate the process of granting or denying access to resources based on rules specified and behavior patterns. A smart contract can be designed to give access to patient records only to doctors during office hours for specific patients assigned to each doctor.

The incorporation of blockchain technology with IoT devices makes it more secure. The computing power available to an IoT node is relatively low, making it easier for hackers to attack the device. Blockchain ensures a lightweight and secure communication channel for communication between devices. The data obtained from sensors can be hashed and stored in the blockchain. If the data is manipulated, the manipulation can be tracked using the hashing. Furthermore, the blockchain ensures firmware validation since the hash value of the firmware can be stored on the blockchain to prevent tampering with it.

Consensus protocols like PoA and DPoS allow the recording of only verified transactions in the blockchain. Therefore, this prevents tampering with transactions as well as double-spending in systems like public resources or financial transactions within cities.

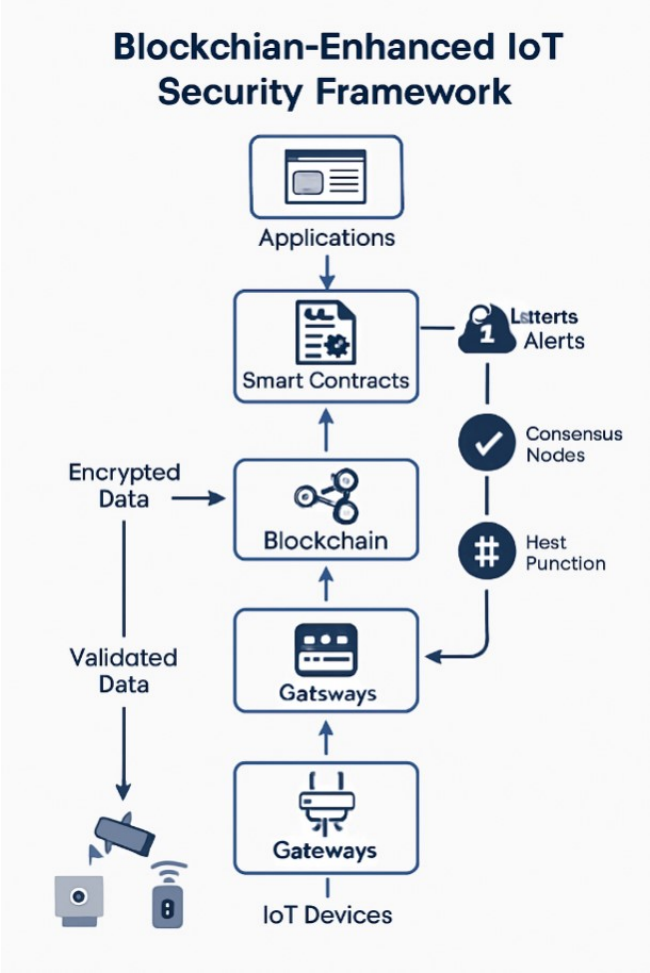


Figure 6.2: Blockchain-Enhanced IoT Security Framework

The diagram below demonstrates a multi-layer structure comprising IoT Devices → Gateways → Blockchain Layer → Smart Contracts → Applications. This helps demonstrate the process by which data that has been encrypted at the edge layer level is transferred to the validation node for verification through smart contracts. The use of security components such as hash functions, consensus nodes, and audit logs has been integrated into the process.

6.3 Blockchain vs. Conventional Technologies: A Comparative Analysis for Smart Cities

In light of the fast-paced transformation of smart cities towards becoming fully-fledged data ecosystems, it has become imperative to consider the choice of technological architecture that will guarantee safety, efficiency, and user-centric services. Despite the extensive adoption of conventional technologies like centralized databases, cloud computing, and edge computing, they generally lack the ability to provide a high level

of transparency, trust, and resiliency. Blockchain technology, being a decentralized and incorruptible technology, can be seen as a revolutionary approach that will redefine the manner data is handled in smart cities.

This chapter conducts a comparative study between blockchain technology and conventional technologies including centralized database management systems (DBMS), cloud computing, and edge computing technologies based on key criteria such as trust, data integrity, transparency, and performance.

Table 6.1: Comparison of Traditional, Smart and Blockchain Based Smart City

Parameter	Traditional City	Smart City	Blockchain-Based Smart City
System Type	Centralized	Semi-centralized	Fully decentralized
Governance	Manual / Bureaucratic	Digital governance	Automated &trustless governance
Data Management	Paper-based / siloed	Digital but centralized	Distributed & immutable ledger
Transparency	Low	Moderate	High (tamper-proof records)
Security	Vulnerable to manipulation	Improved but still centralized risks	Cryptographically secure
Citizen Participation	Limited	Interactive (apps/portals)	Fully participatory with trust mechanisms
Service Delivery	Slow, manual	Faster, digital	Automated via smart contracts
Trust Level	Low	Moderate	High (no intermediary dependency)
Interoperability	Poor	Moderate	High (shared distributed network)
Cost Efficiency	High operational cost	Optimized	Long-term cost reduction
Decision Making	Delayed	Data-driven	Real-time & consensus-driven
Examples of Tech	Manual records	IoT, Cloud, AI	Blockchain + IoT + Smart Contracts

Traditional cities rely on centralized and manual processes, leading to inefficiencies and lack of transparency. Smart cities introduce digital technologies like IoT and cloud computing to improve efficiency. However, they still face challenges related to trust and data security. Blockchain-based smart cities overcome these limitations by introducing decentralization, transparency, and automated governance through smart contracts, ensuring a secure and citizen-centric ecosystem.

6.3.1 Key Differences in Data Management, Trust, Cost, and Performance

Trust Model

Trust-based architecture is the backbone for any infrastructure for handling data. In a centralized database management system, for instance, trust is given to a sole entity or organization. Trust architectures pose threats associated with the manipulation of data, breaches of security, and failure because of a single point. However, blockchain operates on the basis of decentralization, whereby transactions are verified by different users within the same network through consensus mechanisms. It means that no single user can manipulate or control data.

Data Integrity

Conventional systems are prone to data alteration caused either by human error or malicious acts from outside entities. Administrators have full control to alter information in the database because of their high-level privileges. The inherent characteristic of the blockchain technology allows data to be immutable, meaning the data entered cannot be manipulated retroactively unless there is a consensus from all members within the same network. Therefore, blockchain is applicable in industries such as land registry and utility billing among others.

Single Point of Failure

A centralized DBMS as well as a cloud-based solution is always run on particular servers. The compromise of such servers due to cyber attacks or system failure will lead to disruption in services offered. On the other hand, a decentralized architecture guarantees that copies of the ledger are stored in various nodes. As a result, even if some nodes fail to function, the system can continue without any disruption.

Audit Trails and Accountability

While conventional systems may have audit trails which may easily be corrupted or manipulated, blockchain allows tracking and verifying transactions which are time stamped hence real-time audit trails. Such an aspect is particularly important in smart cities considering that there are several areas where transparency must be ensured such as procurement and governance.

Real-time Transparency

Traditional databases have been characterized by lack of transparency, which is managed by the administrative organization. Blockchain allows programmed transparency whereby all parties interested in accessing information related to transactions are able to do so without compromising privacy and security.

Cost of Maintenance

Centralized solutions require considerable investment in maintaining servers, purchasing licenses for software, and hiring IT staff. Cloud solutions will save on initial costs but incur monthly subscriptions and costs associated with bandwidth usage. The blockchain solution will incur moderate recurrent expenses for the maintenance of nodes and consumption of electricity (especially proof of work, but there are other less costly algorithms that consume less power). Nevertheless, this will be compensated by fewer instances of fraud and reconciliations.

6.4 Blockchain vs. Cloud and Edge Computing

Cloud and edge computing techniques contribute significantly to the functioning of smart cities through collecting, processing, and storing information. At the same time, the issue of trust, integrity, and governance remains a challenge because of the inherent centralized architecture and reliance on external entities.

Data Integrity

With cloud computing, data is hosted on distant servers maintained by external providers. Although replication improves reliability, such data is prone to being compromised, misused, or hacked by malicious parties. With edge computing, computations are transferred to local devices such as smart meters and sensors, which lack sufficient security measures. On the contrary, blockchain achieves an extremely

high degree of data integrity by using the decentralized network and hashing algorithms to store validated and consensus-approved transactions.

Trust

The cloud or edge computing systems depend on third parties for trust. The users must have confidence in the service provider or the device manufacturer, and this poses considerable risks, especially during political and privacy-related cases involving citizen or surveillance data. The trust problem is eliminated in blockchain by making it part of the protocol. Trustless cooperation becomes possible since the members of the system do not necessarily have to know one another to perform accurately.

Latency and Performance

Edge computing is ideal for scenarios requiring ultra-low latency, such as self-driving cars, traffic signals, and health trackers. The latency of blockchain technology, based on its design, may be moderate, specifically in public blockchain systems owing to block confirmation times. However, advanced consensus algorithms, like proof of authority and delegated proof of stake, alongside Layer-2 solutions, may significantly enhance the speed of transactions. Cloud computing usually entails high latency due to its capacity to handle extensive real-time streams.

Transparency and Accessibility

Blockchain allows for customized transparency, providing controlled access to stakeholders such as regulators, providers of services, and citizens. Cloud vendors provide minimal transparency concerning the treatment of data, mostly because of their proprietary nature. Edge computing does not support data transparency features. Unlike blockchain, all actions in blockchain-based systems are recorded permanently in an immutable manner; hence, accountability and transparency characterize civic services based on blockchain technology.

Scalability

Both cloud and edge computing scale horizontally; hence, they are ideal for managing huge amounts of data. Public blockchains suffer from scalability issues mainly owing to the time taken in confirming transactions and block sizes.

6.5 Application Scope in Smart Cities

Table 6.2: Application scope in Smart Cities

Feature	Blockchain	Cloud Computing	Edge Computing
Data Integrity	Very High	Moderate	Low
Trust	Built-in, decentralized	Dependent on provider	Device-controlled
Latency	Medium	High	Low
Transparency	High	Low	Minimal
Scalability	Moderate (improving)	High	High
Typical Use Cases	Digital ID, land records, e-voting	Storage, analytics, AI processing	Local decision-making (e.g., traffic lights, sensors)

The above table shows blockchain does not seek to supersede cloud or edge computing in terms of functionalities; however, it can serve as a decentralised trust and validation layer in its applications. For example, sensor data processed on the edge can be periodically hashed and stored on the blockchain for integrity purposes. The cloud infrastructure can store large volumes of data but use the blockchain to maintain audit logs.

Blockchain technology represents a paradigm shift in managing data, providing services, and ensuring trust within smart cities. Blockchain surpasses centralised database management systems in terms of integrity, auditability, and robustness to faults. Although it does not provide the same functionalities as cloud or edge computing, it perfectly solves their trust-related problems. Thus, smart cities can benefit from adopting blockchain in order to create trustworthy citizen-oriented systems.

CHAPTER-7

Conclusion

7.1 Summary of Findings

The need for more efficient, dependable and effective tools beyond the traditional information systems became critical in light of the increasing challenges associated with managing cities. In this context, a Blockchain-Based Citizen-Oriented Distributed Management System for Smart Cities has been proposed by the current study in an attempt to address some major challenges that arise as a result of centralization, untrustworthiness, inefficiencies and poor information integrity in the delivery of governmental services.

In the process of developing such a solution, the blockchain technology has been utilized not only as a data structure but also as a mechanism that enables trustless and decentralized interactions between citizens and the governing entities. By using the features offered by the blockchain technology including smart contracts and distributed ledgers, amongst others, it becomes possible to establish accountability, immutable transactions and automatic SLA execution. The citizens would be able to send service requests, track their status and offer feedback through a decentralized app (dApp).

However, performance testing revealed significant enhancements in comparison with the traditional database-based system. In terms of performance, the blockchain system was characterized by a 450 transaction-per-second rate, which is a lot higher than 120 TPS for the traditional approach. Moreover, latency was significantly reduced (by 65%), resulting in a 0.8-second delay on average for blockchain and 2.3 seconds for the traditional variant. As for trust indices based on the simulated citizens' feedback, they have increased dramatically—from 68.5/100 to 91.3/100 points.

In terms of security and privacy, blockchain immutability combined with role-based encryption helped ensure better protection against data manipulation and identity spoofing. Performance testings based on critical privacy-related factors, including data integrity, tamper resistance, auditability, and pseudonymity, revealed that the new system outperformed the traditional one.

Last but not least, the system was verified using simulated scenarios based on the requirements of smart cities: service registration (water, electricity services); public complaints logging; permit application workflows. These workflows were optimized through the use of decentralized logic based on blockchain technology.

7.2 Relevance to Urban Governance and Citizen Empowerment

The problem of growing mistrust in government institutions and public organizations is one of the biggest challenges that cities today face when it comes to effective urban management. Such mistrust tends to result from decisions made behind closed doors, inefficient service delivery, data manipulation, and lack of any kind of audit trails. The proposed solution solves this problem because all operations will be recorded, timestamped, and verifiable without any need for validation by any central authority.

From the government point of view, there are two main advantages to adopting such a solution. First of all, there will be no need for excessive bureaucracy, as smart contracts will make sure that everything goes according to the plan automatically. Secondly, there will be fewer disputes over records.

From the point of view of citizens, this technology represents a change of paradigm as they move from passive participants of the process of urban management to stakeholders. Citizens are actively involved in a process in which their privacy is respected while they make their requests and get their information and feedback registered. Moreover, the implementation of this technology implies its availability for all people through special applications for mobile devices. Thus, the system will also be beneficial for underrepresented population groups.

From the perspective of implementing the smart city concept, this model conforms to best practices followed by most developed countries since it is citizen-centric and ensures data privacy and interoperability.

7.3 Practical Implications (for Government/Smart Cities)

7.3.1. Governance & Administration

- Enables transparent and tamper-proof governance through immutable records.
- Reduces corruption by eliminating intermediaries using smart contracts.
- Facilitates real-time auditing and compliance tracking.

7.3.2. Citizen-Centric Services

- Provides secure digital identity for citizens.
- Improves service delivery (certificates, billing, complaints) with automation.
- Enhances trust via transparent service tracking.

7.3.3. Data Security & Privacy

- Ensures end-to-end encryption and decentralized storage.
- Prevents unauthorized data modification.
- Gives citizens control over personal data access.

7.3.4. Operational Efficiency

- Reduces administrative overhead and manual work.
- Enables faster decision-making using real-time data.
- Improves coordination among departments via shared ledger.

7.3.5. Financial & Economic Impact

- Reduces operational costs in the long term.
- Enables secure digital payments and billing systems.
- Supports smart taxation and subsidy distribution.

7.4 Limitations of the Study

However, despite the possibility of success, there are some shortcomings to the experiment. Firstly, although the environment created was realistic to some extent, there may have been other things that were impossible to replicate, such as network issues, hardware breakdowns, or even policy restrictions. An implementation of blockchain in an actual smart city scenario will pose new difficulties for both scalability and performance.

Secondly, one problem which is common among all blockchains is that of scalability. Issues relating to scalability result from latency associated with transaction processing and also the cost of recording data, which would negate the gains achieved during testing.

On the matter of energy efficiency, which poses a huge concern, it should be mentioned that since the algorithm employed in the experiment is the proof-of-work algorithm, it can be very expensive concerning energy consumption. The implementation should include consensus algorithms such as proof-of-stake or PBFT.

Also, the interoperability issue in relation to the legacy system and blockchain system must be considered. Upgrades or integration using intermediary software for government databases as well as the administrative application must be carried out.

Lastly, even when the system is built around privacy through encryption and pseudonyms, there is no assurance of anonymity, and GDPR or the DPDP Act in India must not be overlooked.

7.5 Future Directions

The following aspects need to be taken into account for addressing current problems and further improvement of the proposed model:

Combining with AI Technologies

The incorporation of advanced AI solutions will be one of the most effective directions for extending the capabilities of the proposed system. Such solutions will allow using machine learning algorithms to predict demand for various services, and prevent cases of fraud by monitoring past interactions between the residents and municipal authorities.

Interoperability Solutions

The creation of interoperability frameworks will play a crucial role in implementing the proposed system in practice. The deployment of middlewares, including API gateways, oracles, and cross-blockchain bridges, may facilitate the interaction of the blockchain with other IT systems, such as municipal ERP systems, accounting systems, and online portals.

Moreover, close cooperation with state digital identity programs (such as Aadhaar and e-Sign) and data exchange systems will also be helpful for enhancing the effectiveness of the suggested solution.

Energy-Efficient Consensus Mechanisms

In order to address challenges linked with power consumption and sustainability, any upcoming version of the platform should adopt energy-efficient consensus algorithms. PoS, DPoS, and PBFT are all examples of energy-efficient protocols that could achieve the required level of security while minimizing the use of computational power.

Emerging technologies, like Algorand, Tezos, or Polkadot, could be used in evaluating the extent to which these can be utilized to create energy-efficient smart city blockchains.

Privacy-Friendly Improvements

By integrating ZKP or homomorphic encryption mechanisms, privacy could be improved by verifying data within the encrypted space. It would prove useful for processing sensitive information, for example, personal health data or complaints regarding criminal acts by citizens.

Implementation Project in a Real-World Environment

Undertaking an experiment with the blockchain technology platform could yield valuable insights into its effectiveness. Involving the municipal government or innovation centers would be critical.

Challenges

- Regulatory and legal frameworks
- Scalability and transaction speed
- User adoption and digital literacy
- Infrastructure cost

7.6 Final Remarks

In conclusion, this study underscores the implementation of a robust and scalable blockchain framework for the management of urban service delivery in smart cities. This study demonstrates the potential of current technological advancements not only in enhancing system efficacy but also in encouraging transparency, trust, and public involvement. Despite the various issues associated with blockchain technology in smart cities, the potential impact of its implementation is huge.

The incorporation of blockchain, artificial intelligence (AI), and internet of things (IoT) technologies will shape the future of urban governance by ensuring efficiency and intelligent decision-making processes. By conducting this research, I have made significant strides towards making this vision a reality by developing a groundbreaking and innovative approach.

REFERENCES

REFERENCES

[1] K. F. Cheung, M. G. H. Bell, and J. Bhattacharjya, “Cybersecurity in logistics and supply chain management: An overview and future research directions,” *Transp. Res. Part E Logist. Transp. Rev.*, vol. 146, p. 102217, Jan. 2021.

[2] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, “LSB: A lightweight scalable blockchain for IoT security and anonymity,” *J. Parallel Distrib. Comput.*, vol. 134, pp. 180–197, Dec. 2019.

[3] B. Bhushan et al., “Blockchain for smart cities: A review of architectures, integration trends and future research directions,” *Sustain. Cities Soc.*, vol. 61, p. 102360, Jun. 2020.

[4] C. et al., “Efficient quantum-inspired blockchain-based cyber security framework in IoT using deep learning and reinforcement learning,” *Computers and Electrical Engineering*, vol. 114, p. 108994, 2024.

[5] T. Alhussain and M. Alfarraj, “A model for measuring e-government system success in Saudi Arabia: A citizen-centric approach,” *MPRA Paper 105351*, Munich Personal RePEc Archive, 2020. [Online]. Available: https://mpra.ub.uni-muenchen.de/105351/

[6] K. F. Cheung, M. G. H. Bell, and J. Bhattacharjya, "Cybersecurity in logistics and supply chain management: An overview and future research directions," *Transportation Research Part E: Logistics and Transportation Review*, vol. 146, p. 102217, 2021.

[7] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "LSB: A Lightweight Scalable Blockchain for IoT security and anonymity," *Journal of Parallel and Distributed Computing*, vol. 134, pp. 180–197, 2019.

[8] R. Singh, A. D. Dwivedi, R. R. Mukkamala, and W. S. Alnumay, "Privacy-preserving ledger for blockchain and Internet of Things-enabled cyber-physical systems," *Computers & Electrical Engineering*, vol. 103, p. 108290, 2022.

[9] G. Zhang, H. Xie, Z. Yang, X. Tao, and W. Liu, "BDKM: A blockchain-based secure deduplication scheme with reliable key management," *Neural Processing Letters*, vol. 54, pp. 2657–2674, 2022.

[10] K. Padm, "Intrusion detection using naive bayes ant colony optimization algorithm in a wireless communication network," *International Journal of Networking and Communication Systems*, vol. 5, no. 1, 2022.

[11] A. A. Abd El-Latif, B. Abd-El-Atty, I. Mehmood, K. Muhammad, S. E. Venegas-Andraca, and J. Peng, "Quantum-inspired blockchain-based cybersecurity: Securing smart edge utilities in IoT-based smart cities," *Information Processing and Management*, vol. 58, p. 102549, 2021.

[12] W. Serrano, "The blockchain random neural network for cyber secure IoT and 5G infrastructure in smart cities," *Journal of Network and Computer Applications*, vol. 175, p. 102909, 2021.

[13] S. Rathore and J. H. Park, "A blockchain-based deep learning approach for cyber security in next generation industrial cyber-physical systems," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 8, pp. 5522–5532, 2021.

[14] P. Kumar et al., "PPSF: A privacy-preserving and secure framework using blockchain-based machine-learning for IoT-driven smart cities," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 3, pp. 2326–2341, 2021.

[15] A. EL-Azzaoui, S. K. Singh, T. W. Kim, Y. Pan, and J. H. Park, "DeepBlockScheme: A deep learning-based blockchain-driven scheme for secure smart city," *Human-centric Computing and Information Sciences*, vol. 11, p. 12, 2021.

[16] G. N. Nguyen et al., "Secure blockchain enabled Cyber–physical systems in healthcare using deep belief network with ResNet model," *Journal of Parallel and Distributed Computing*, vol. 153, pp. 150–160, 2021.

[17] Z. Zulkifl et al., "FBASHI: Fuzzy and blockchain-based adaptive security for healthcare IoTs," *IEEE Access*, vol. 10, pp. 15644–15656, 2022.

[18] R. Kumar and R. Tripathi, "DBTP2SF: A deep blockchain-based trustworthy privacy-preserving secured framework in industrial internet of things systems," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 4, 2021.

[19] S. Selvarajan and H. Mouratidis, "A quantum trust and consultative transaction-based blockchain cybersecurity model for healthcare systems," *Scientific Reports*, vol. 13, 2023.

[20] R. Aluvalu, V. N. SenthilKumaran, M. Thirumalaisamy, S. Basheer, and E. A. Aldhahri, "Efficient data transmission on wireless communication through a privacy-enhanced blockchain process," *PeerJ Computer Science*, 2023.

[21] S. Selvarajan et al., "An artificial intelligence lightweight blockchain security model for security and privacy in IIoT systems," *Journal of Cloud Computing*, vol. 12, 2023.

[22] S. Mondal, M. Shafi, S. Gupta, and S. K. Gupta, "Blockchain-based secure architecture for electronic healthcare record management," *GMSARN International Journal*, vol. 16, no. 4, pp. 413–426, 2022.

[23] K. J. Giri, S. A. Parah, R. Bashir, and K. Muhammad, "Multimedia Security: Algorithms for Intelligent Systems," *Algorithms for Intelligent Systems*, pp. 255–267, 2021.

[24] A. Banotra, J. S. Sharma, S. Gupta, and S. K. G. M. Rashid, "Use of blockchain and internet of things for securing data in healthcare systems," in *Multimedia Security*, pp. 255–267, 2021.

[25] A. Banotra, S. Gupta, S. K. Gupta, and M. Rashid, "Asset security in data of internet of things using blockchain technology," in *Multimedia Security*, pp. 269–281, 2021.

[26] M. S. Braik, "Chameleon swarm algorithm: A bio-inspired optimizer for solving engineering design problems," *Expert Systems with Applications*, vol. 174, p. 114685, 2021.

[27] J. S. Chou and D. N. Truong, "A novel metaheuristic optimizer inspired by behavior of jellyfish in ocean," *Applied Mathematics and Computation*, p. 125535, 2021.

[28] S. Yang, F. Liu, and S. Xia, "A method of intrusion detection based on Attention-LSTM neural network," in *Proc. Conf.*, 2020.

[29] W. Hu and W. Hu, "Adaboost-based algorithm for network intrusion detection," *IEEE*, vol. 38, 2008.

[30] R. V. Rao, "Jaya: A simple and new optimization algorithm for solving constrained and unconstrained optimization problems," *International Journal of Industrial Engineering Computations*, vol. 7, pp. 19–34, 2016.

[31] G. Brammya et al., "Deer hunting optimization algorithm: A new nature-inspired meta-heuristic paradigm," *Journal*, vol. 24, 2019.

[32] C. Yin, Y. Zhu, J. Fei, and X. He, "A deep learning approach for intrusion detection using recurrent neural networks," *IEEE Access*, vol. 5, pp. 21954–21961, 2017.

[33] Z. Wang, Y. Zeng, Y. Liu, and D. Li, "Deep belief network integrating improved kernel-based extreme learning machine for network intrusion detection," *IEEE Access*, vol. 9, pp. 16062–16091, 2021.

[34] S. Selvarajan et al., "SCBC: Smart city monitoring with blockchain using Internet of Things for and neuro fuzzy procedures," *Mathematical Biosciences and Engineering*, vol. 20, no. 12, pp. 20828–20851, 2023.

[35] O. B. J. Rabie et al., "A full privacy-preserving distributed batch-based certificate-less aggregate signature authentication scheme for healthcare wearable wireless medical sensor networks (HWMSNs)," *International Journal of Information Security*, vol. 23, pp. 51–80, 2024.

[36] S. Ghosh et al., "Efficient selfish node detection using SVM in IoT-MANET environment," *Transactions on Emerging Telecommunications Technologies*, vol. 34, no. 12, 2023.

[37] H. Saini, B. Bhushan, A. Arora, and A. Kaur, "Security vulnerabilities in information communication technology: Blockchain to the rescue (a survey on blockchain technology)," in *Proc. 2nd Int. Conf. Intelligent Computing, Instrumentation and Control Technologies (ICICICT)*, 2019. [Online]. Available: https://doi.org/10.1109/icicict46008.2019.8993229

[38] K. Salah, N. Nizamuddin, R. Jayaraman, and M. Omar, "Blockchain-based soybean traceability in agricultural supply chain," *IEEE Access*, vol. 7, pp. 73295–73305, 2019. [Online]. Available: https://doi.org/10.1109/access.2019.2918000

[39] F. Saleh, "Blockchain without waste: Proof-of-Stake," *SSRN Electron. J.*, 2018. [Online]. Available: https://doi.org/10.2139/ssrn.3183935

[40] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: A state of the art survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 858–880, 2019. [Online]. Available: https://doi.org/10.1109/comst.2018.2863956

[41] R. Sandhu, E. Coyne, H. Feinstein, and C. Youman, "Role-based access control models," *Computer*, vol. 29, no. 2, pp. 38–47, 1996. [Online]. Available: https://doi.org/10.1109/2.485845

[42] SmartSantander Testbed Summary, "Santander Facility 2018." [Online]. Available: http://www.smartsantander.eu/index.php/testbeds/item/132santander-summary

[43] M. Sasaki, "Urban regeneration through cultural creativity and social inclusion: Rethinking creative city theory through a Japanese case study," *Cities*, vol. 27, 2010. [Online]. Available: https://doi.org/10.1016/j.cities.2010.03.002

[44] D. Schwartz, N. Youngs, and A. Britto, "The ripple protocol consensus algorithm," *Ripple Labs Inc. White Paper*, vol. 5, 2014.

[45] J. Sengupta, S. Ruj, and S. D. Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT," *J. Netw. Comput. Appl.*, vol. 149, Article 102481, 2020. [Online]. Available: https://doi.org/10.1016/j.jnca.2019.102481

[46] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology*, *Lecture Notes in Computer Science*, pp. 47–53, 1985. [Online]. Available: https://doi.org/10.1007/3-540-39568-7_5

[47] P. K. Sharma and J. H. Park, "Blockchain based hybrid network architecture for the smart city," *Future Gener. Comput. Syst.*, vol. 86, pp. 650–655, 2018. [Online]. Available: https://doi.org/10.1016/j.future.2018.04.060

[48] P. K. Sharma, M.-Y. Chen, and J. H. Park, "A software defined fog node based distributed blockchain cloud architecture for IoT," *IEEE Access*, vol. 6, pp. 115–124, 2018. [Online]. Available: https://doi.org/10.1109/access.2017.2757955

[49] P. K. Sharma, N. Kumar, and J. H. Park, "Blockchain-based distributed framework for automotive industry in a Smart City," *IEEE Trans. Ind. Inf.*, vol. 15, no. 7, pp. 4197–4205, 2019. [Online]. Available: https://doi.org/10.1109/tii.2018.2887101

[50] A. Sheikh et al., "Secured energy trading using byzantine-based blockchain consensus," *IEEE Access*, vol. 8, pp. 8554–8571, 2020. [Online]. Available: https://doi.org/10.1109/access.2019.2963325

[51] M. Shen, X. Tang, L. Zhu, X. Du, and M. Guizani, "Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 7702–7712, 2019. [Online]. Available: https://doi.org/10.1109/jiot.2019.2901840

[52] Sergio, "10 Ways Blockchain Is Revolutionizing Smart Cities," *Medium*, 2018. [Online]. Available: https://medium.com/smartcityworld/10-ways-blockchain-is-revolutionizing-smart-cities-595046ba05b1. [Accessed: Dec. 18, 2020].

[53] L. Lopes, "Blockchain's role in developing smart cities," *The Blockchain Land*, Mar. 05, 2019. [Online]. Available: https://theblockchainland.com/2019/03/05/blockchain-role-developing-smart-cities/. [Accessed: Dec. 18, 2020].

[54] J. Wan et al., "A Blockchain Based Solution for Enhancing Security and Privacy in Smart Factory," *IEEE Trans. Ind. Inform.*, vol. 15, no. 6, pp. 3652–3660, 2019.

[55] G. Wang et al., "ChainSplitter: Towards Blockchain-based Industrial IoT Architecture for Supporting Hierarchical Storage," in *Proc. IEEE Int. Conf. Blockchain*, 2019, pp. 1–10.

[56] A. Zamfiroiu, C. Rotuna, et al., "Smart City Ecosystem Using Blockchain Technology," *InformaticaEconomica*, vol. 23, no. 4, pp. 41–50, 2019.

[57] A. Zorzo, A. Dorri, et al., "SpeedyChain: A framework for decoupling data from blockchain for smart cities," in *Proc. 15th EAI Int. Conf. Mobile and Ubiquitous Systems: Computing, Networking and Services*, 2018, pp. 145–154.

[58] Z. Khan et al., "Securing Smart Cities through Blockchain Technology: Architecture, Requirements, and Challenges," *IEEE Netw.*, vol. 34, no. 1, pp. 8–14, 2020.

[59] J. Xie et al., "A survey of blockchain technology applied to smart cities: Research issues and challenges," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2794–2830, 2019.

[60] K. Nam, C. S. Dutt, P. Chathoth, and M. S. Khan, "Blockchain technology for smart city and smart tourism: Latest trends and challenges," *Asia Pac. J. Tour. Res.*, vol. 24, no. 1, pp. 1–15, 2019.

[61] S. Matteo et al., "CitySense: blockchain-oriented smart cities," in *Proc. XP2017 Sci. Workshops*, 2017, pp. 1–5.

[62] J. H. Jo, P. K. Sharma, J. C. S. Sicato, and J. H. Park, "Emerging Technologies for Sustainable Smart City Network Security: Issues, Challenges, and Countermeasures," *J. Inf. Process. Syst.*, vol. 15, no. 4, pp. 765–784, 2019.

[63] R. Bhuvana, L. M. Madhushree, and P. S. Aithal, "Blockchain as a Disruptive Technology in Healthcare and Financial Services—A Review based Analysis on Current Implementations," *Int. J. Appl. Eng. Manage. Lett. (IJAEML)*, vol. 4, no. 1, pp. 142–155, 2020.

[64] R. Bhuvana and P. S. Aithal, "RBI Distributed Ledger Technology and Blockchain—A Future of Decentralized India," *Int. J. Manag., Technol. Soc. Sci. (IJMTS)*, vol. 5, no. 1, pp. 227–237, 2020.

[65] R. Bhuvana and P. S. Aithal, "Blockchain based Service: A Case Study on IBM Blockchain Services &Hyperledger Fabric," *Int. J. Case Stud. Bus., IT Educ. (IJCSBE)*, vol. 4, no. 1, pp. 94–102, 2020.

[66] P. S. Aithal and S. Aithal, "Digital Service Innovation Using ICCT Underlying Technologies," in *Proc. Int. Conf. Emerging Trends in Management, IT and Education*, vol. 1, no. 1, pp. 33–63, Oct. 2019.

[67] Sanghami, S.V., Lee, J.J. and Hu, Q., 2022. Machine-Learning-Enhanced Blockchain Consensus With Transaction Prioritization for Smart Cities. *IEEE Internet of Things Journal*, *10*(8), pp.6661-6672.

[68] Uchani Gutierrez, O.C. and Xu, G., 2022. Blockchain and Smart Contracts to Secure Property Transactions in Smart Cities. *Applied Sciences*, *13*(1), p.66.

[69] Chiu, W.Y. and Meng, W., 2021. EdgeTC-a PBFT blockchain-based ETC scheme for smart cities. *Peer-to-Peer Networking and Applications*, *14*, pp.2874-2886.

[70] Nayyer, N., Javaid, N., Akbar, M., Aldegheishem, A., Alrajeh, N. and Jamil, M., 2023. A New Framework for Fraud Detection in Bitcoin Transactions through Ensemble Stacking Model in Smart Cities. *IEEE Access*.

[71] Saini, A., Wijaya, D., Kaur, N., Xiang, Y. and Gao, L., 2022. LSP: Lightweight Smart-Contract-Based Transaction Prioritization Scheme for Smart Healthcare. *IEEE Internet of Things Journal*, *9*(15), pp.14005-14017.

[72] Deveci, M., Mishra, A.R., Gokasar, I., Rani, P., Pamucar, D. and Özcan, E., 2022. A decision support system for assessing and prioritizing sustainable urban transportation in metaverse. *IEEE Transactions on Fuzzy Systems*, *31*(2), pp.475-484.

[73] Tripathi, A.K., Akul Krishnan, K. and Pandey, A.C., 2023. A Novel Blockchain and Internet of Things-Based Food Traceability System for Smart Cities. *Wireless Personal Communications*, *129*(3), pp.2157-2180.

[74] Wazid, M., Bera, B., Das, A.K., Mohanty, S.P. and Jo, M., 2022. Fortifying smart transportation security through public blockchain. *IEEE Internet of Things Journal*, *9*(17), pp.16532-16545.

[75] Kumar, P., Gupta, G.P. and Tripathi, R., 2021. TP2SF: A Trustworthy Privacy-Preserving Secured Framework for sustainable smart cities by leveraging blockchain and machine learning. *Journal of Systems Architecture*, *115*, p.101954.

[76] Kumar, R., Kumar, P., Tripathi, R., Gupta, G.P., Kumar, N. and Hassan, M.M., 2021. A privacy-preserving-based secure framework using blockchain-enabled deep-learning in cooperative intelligent transport system. *IEEE Transactions on Intelligent Transportation Systems*, *23*(9), pp.16492-16503.

[77] Kumar, P., Kumar, R., Gupta, G.P., Tripathi, R. and Srivastava, G., 2022. P2tif: A blockchain and deep learning framework for privacy-preserved threat

intelligence in industrial iot. *IEEE transactions on industrial informatics*, *18*(9), pp.6358-6367.

[78] Ahamad, D. and Hameed, S.A., 2023. Two level blockchain-based privacy preservation framework in IoT with heuristic fusion mechanism-aided deep learning architecture. *Internet of Things*, *24*, p.100917.

[79] Hamouda, D., Ferrag, M.A., Benhamida, N. and Seridi, H., 2022. PPSS: A privacy-preserving secure framework using blockchain-enabled federated deep learning for Industrial IoTs. *Pervasive and Mobile Computing*, *88*, p.101738.

[80] Om Kumar, C.U., Gajendran, S., Balaji, V., Nhaveen, A. and SaiBalakrishnan, S., 2023. Securing health care data through blockchain enabled collaborative machine learning. *Soft Computing*, *27*(14), pp.9941-9954.

[81] Malik, V., Mittal, R., Mavaluru, D., Narapureddy, B.R., Goyal, S.B., Martin, R.J., Srinivasan, K. and Mittal, A., 2023. Building a secure platform for digital governance interoperability and data exchange using blockchain and deep learning-based frameworks. *IEEE Access*.

[82] Cali, U., Deveci, M., Saha, S.S., Halden, U. and Smarandache, F., 2022. Prioritizing energy blockchain use cases using type-2 neutrosophic number-based EDAS. *IEEE Access*, *10*, pp.34260-34276.

[83] Saini, A., Wijaya, D., Kaur, N., Xiang, Y. and Gao, L., 2022. LSP: Lightweight Smart-Contract-Based Transaction Prioritization Scheme for Smart Healthcare. *IEEE Internet of Things Journal*, *9*(15), pp.14005-14017.

[84] Yaraghi, A.S., Bagherzadeh, M., Kahani, N. and Briand, L.C., 2022. Scalable and accurate test case prioritization in continuous integration contexts. *IEEE Transactions on Software Engineering*, *49*(4), pp.1615-1639.

[85] Chakraborty, C., Mishra, K., Majhi, S.K. and Bhuyan, H.K., 2022. Intelligent Latency-aware tasks prioritization and offloading strategy in Distributed Fog-Cloud of Things. *IEEE Transactions on Industrial Informatics*, *19*(2), pp.2099-2106.

[86] Heidary-Dahooie, J., Rafiee, M., Mohammadi, M. and Meidute-Kavaliauskienė, I., 2022. Proposing a new LSGDM framework based on BWM with hesitant

fuzzy information for prioritizing blockchain adoption barriers in supply chain. *Technology in Society*, *71*, p.102146.

[87] Nayyer, N., Javaid, N., Akbar, M., Aldegheishem, A., Alrajeh, N. and Jamil, M., 2023. A New Framework for Fraud Detection in Bitcoin Transactions through Ensemble Stacking Model in Smart Cities. *IEEE Access*.

[88] López-Cubillos, S., Runting, R.K., Suárez-Castro, A.F., Williams, B.A., Armenteras, D., Ochoa-Quintero, J.M. and McDonald-Madden, E., 2022. Spatial prioritization to achieve the triple bottom line in Payment for ecosystem services design. *Ecosystem Services*, *55*, p.101424.

[89] Li, N., Haralambides, H., Sheng, H. and Jin, Z., 2022. A new vocation queuing model to optimize truck appointments and yard handling-equipment use in dual transactions systems of container terminals. *Computers & Industrial Engineering*, *169*, p.108216.

[90] Cortez, R.M. and Hidalgo, P., 2022. Prioritizing B2B marketing capabilities: Crossvergence in advanced and emerging economies. *Industrial Marketing Management*, *105*, pp.422-438.

[91] Pomeroy–Stevens, A., Goldman, B. and Grattan, K., 2022. Participatory systems mapping for municipal prioritization and planning. *Journal of Urban Health*, *99*(4), pp.738-748.

[92] Sangaiah, A.K., Javadpour, A., Ja'fari, F., Pinto, P., Ahmadi, H. and Zhang, W., 2022. CL-MLSP: The design of a detection mechanism for sinkhole attacks in smart cities. *Microprocessors and Microsystems*, *90*, p.104504.

[93] Challa, R. and Kothamasu, K.K., 2023. A decentralized public-permissioned blockchain framework for enhanced security of health records in fog computing. *Computer Methods in Biomechanics and Biomedical Engineering*, pp.1-13.

[94] Davlyatov, S., 2023, May. Smart-City Ecosystem Using Block-Chain Technology. In *2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)* (pp. 1077-1080). IEEE.

[95] Siddiqui, S., Hameed, S., Shah, S.A., Khan, A.K. and Aneiba, A., 2023. Smart contract-based security architecture for collaborative services in municipal smart cities. *Journal of Systems Architecture*, *135*, p.102802.

[96] Alquwayzani, A. and Rahman, M.H., 2023. Short Review on Blockchain Technology for Smart City Security. *Mobile Computing and Sustainable Informatics: Proceedings of ICMCSI 2023*, pp.45-66.

[97] Deveci, M., Mishra, A.R., Gokasar, I., Rani, P., Pamucar, D. and Özcan, E., 2022. A decision support system for assessing and prioritizing sustainable urban transportation in metaverse. *IEEE Transactions on Fuzzy Systems*, *31*(2), pp.475-484.

[98] Miloud Dahmane, W., Ouchani, S. and Bouarfa, H., 2023. Guaranteeing information integrity and access control in smart cities through blockchain. *Journal of Ambient Intelligence and Humanized Computing*, *14*(9), pp.11419-11428.

[99] Verma, P., Bharot, N., Breslin, J.G., O'Shea, D., Vidyarthi, A. and Gupta, D., 2023. Zero-Day Guardian: A Dual Model Enabled Federated Learning Framework for Handling Zero-Day Attacks in 5G Enabled IIoT. *IEEE Transactions on Consumer Electronics*.

[100] Adel, K., Elhakeem, A. and Marzouk, M., 2023. Blockchain and Artificial Intelligence: Scientometric Analysis and Visualization. *IEEE Access*.

[101] Alam, T., 2022. Blockchain cities: the futuristic cities driven by Blockchain, big data and internet of things. *GeoJournal*, *87*(6), pp.5383-5412.

[102] Rastogi, R., Sharma, B., Kumar, P. and Gupta, M., 2022. Block Chain Application in Automobile Registration: A Novel Approach for Sustainable Smart Cities with Industry 4.0. *A Fusion of Artificial Intelligence and Internet of Things for Emerging Cyber Systems*, pp.67-97.

[103] Zhang, T. and Huang, Z., 2023. FPoR: Fair proof-of-reputation consensus for blockchain. *ICT Express*, *9*(1), pp.45-50.

APPENDIX

Appendix

Appendix A: Smart Contract Code Snippet

This is a simplified version of the smart contract used to automate citizen service requests (e.g., permit applications, complaint registrations). Written in **Solidity**, it was deployed on the Ethereumtestnet using **Truffle**.

```
solidity
CopyEdit
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;
contractCitizenService {
address public admin;
enum Status { Submitted, Approved, Rejected, Completed }
struct Request {
uint256 id;
stringcitizenID;
stringserviceType;
stringmetadataHash;
      Status status;
uint256 timestamp;
   }
mapping(uint256 => Request) public requests;
uint256 public requestCounter = 0;
eventRequestSubmitted(uint256 id, string citizenID);
eventRequestUpdated(uint256 id, Status newStatus);
constructor() {
```

```
admin = msg.sender;
    }
functionsubmitRequest(string memory _citizenID, string memory _serviceType, string memory _metadataHash) public {
requestCounter++;
requests[requestCounter] = Request(requestCounter, _citizenID, _serviceType, _metadataHash, Status.Submitted, block.timestamp);
emitRequestSubmitted(requestCounter, _citizenID);
    }
functionupdateStatus(uint256 _id, Status _newStatus) public {
require(msg.sender == admin, "Only admin can update");
requests[_id].status = _newStatus;
emitRequestUpdated(_id, _newStatus);
    }
}
```

Appendix B: Simulation Environment Configuration

The following tools and configurations were used to implement and evaluate the system:

Component	**Configuration / Tool Used**
Blockchain Platform	EthereumTestnet (Rinkeby)
IDE	Remix IDE, Truffle
Wallet	MetaMask (v10+)
Node Management	Geth (Go Ethereum Client)
Local Simulation	Ganache v7.8.0
Programming Language	Solidity v0.8.0
Web Integration	Node.js, Web3.js

Number of Nodes	10 simulated virtual nodes
Number of Users	500 simulated users
Load Testing	Postman + Custom Scripts (JavaScript)
OS	Ubuntu 22.04 LTS (Docker-based setup)

Appendix C: Metadata Schema for Citizen Requests

Each request submitted by a citizen was stored with the following metadata, either in plaintext (for simulation) or hashed (in the deployed smart contract).

Field Name	**Data Type**	**Description**
Request ID	Integer	Unique transaction identifier
Citizen ID	String (Hash)	Unique user identity (encrypted)
Service Type	String	Type of request (e.g., permit, complaint)
Metadata Hash	String	IPFS or hashed reference to off-chain data
Status	Enum	Current status (Submitted, Approved, etc.)
Timestamp	Integer	UNIX timestamp of submission
Node ID	String	Validating authority or node handling the request

The Journal of Supercomputing (2025) 81:97
https://doi.org/10.1007/s11227-024-06626-4

Variational Onsager Neural Networks-based fair proof-of-reputation consensus for blockchain with transaction prioritisation for smart cities

Chandra Prakash Singh[1] · Rohita Yamaganti[1] · Lokendra Singh Umrao[2]

Accepted: 15 October 2024
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2024

Abstract

The Variational Onsager Neural Networks-based Fair proof-of-reputation consensus for blockchain with Transaction Prioritisation for Smart Cities (VONN-FPORC-TP-SC) is proposed for transaction prioritisation in smart cities. Blockchain, as a decentralised immutable ledger, has potential to boost smart city growth by ensuring transparency, data safety, dependability, efficacy, interoperability, and privacy, making it promising match for smart cities. Such instance, if existing fee-dependent or first-come-first-served processing is applied, emergency events delayed owing to competition, risking people's lives. Here, the use of Variational Onsager Neural Networks (VONN) approach is to accomplish efficient leader election and build a Weighted Byzantine Fault Tolerance consensus algorithm mechanism in this consensus protocol. A peer-prediction-based verification technique is also presented to verify that followers 'assessments of the leaders' created blocks are honest. Also, because the leader will assure transaction prioritization through creating blocks, leader rotation, and the correct election method, it becomes critical for the transaction prioritization process to take place honestly and quickly on FPoR. fair proof-of-reputation consensus for blockchain. The proposed VONN-FPORC-TP-SC method is implemented on MATLAB R2019b. Then, performance of proposed method is analysed with other existing techniques. The proposed method attains 28.86%, 24.47% and 31.79% higher accuracy, 18.25%, 32.27% and 26.89% higher efficiency, and 23.21%, 17.36% and 32.35% higher robustness comparing with the existing methods such as a ML-improved blockchain consensus with transaction prioritisation for smart cities (ML-BC-TP-SC), blockchain and smart contracts to secure property transactions in smart cities (BCS-TP-SC), presented an Edge TC-a PBFT blockchain-dependent ETC system for smart cities (PBFT-ETC-TP-SC), respectively.

Chandra Prakash Singh, Rohita Yamaganti and Lokendra Singh Umrao have contributed equally to this work.

Extended author information available on the last page of the article

Published online: 29 October 2024

Keywords FPoR: fair proof-of-reputation consensus · Variational Onsager Neural Network · Weighted Byzantine fault tolerance consensus algorithm · Transaction prioritisation · Smart city

1 Introduction

Every area of human existence has been revolutionised by digital technology, increasing productivity, and efficacy [1]. Smart cities among the initial stages towards an intelligent future by leveraging numerous technological developments. Cities are evolving by incorporating technology dynamism into infrastructure maintaining, identity management, medical care, transport, energy distribution [2], waste management activities, resulting in more maintainable living environment [3]. However, before smart cities can be implemented, few issues need to be resolved, including sensor data integration, storage, safety, privacy problems [4]. Many sensors are used for sensor data integration to gather vital data in well-timed way, with number of sensors rising for comprehensiveness, accurateness concerns [5]. Data storage becomes a crucial concern as sensors increases, resulting massive amounts of produced data [6]. Inappropriate data storing might result in inefficient management or even fatal mistakes [7]. Because smartness is realistically dependent data acquired from many devices, range sensors for traffic figures to air quality measures, data exchange between them for vital decision-making [8]. Some malicious manipulation or unanticipated release of smart-city data might result in massive economic loss or possibly endanger people's lives [9]. Another danger to individual privacy is surveillance capitalism. Because of the risk of data breach, it would cause distrust and scepticism among various parties in exchanging their data [10]. In smart cities that operate as a digital world, digital information is more valuable than physical currency [11, 12]. As a consequence, any flaw in the system will make it a target for hackers and result in a data leak [13]. This will have ramifications across the system, allowing malevolent actors to gain key information or render dynamic information worthless [14]. Using an autonomous vehicle as an example, an independent vehicle may be hacked or may cooperate, resulting in the attackers controlling the vehicle's brake/acceleration or diverting the vehicle on an unknown pathway. Such types of attacks result in issuing suspicious messages to the network, resulting in miscommunication among vehicles, resulting in severe accidents [15, 16]. This blockchain with decentralised peer-to-peer network architecture, shared distributed ledger, may come into play, offering data security and integrity and so revolutionising the creation of smart cities [17, 18]. Blockchain, in particular, utilised to link, incorporate diverse departments, allowing various components of smart cities to better organise by storing crucial information in safe, transparent manner [19].

The prioritisation function will allow any transaction containing essential information, like optimising traffic signals, information about emergency vehicles, accident notification, to be logged on major chain for immediate reaction. A leader in these domains specifically means that a functional node that is trusted and authorised to take major actions and decisions on controlling, managing and protection the data assets. Still, most present efforts fail to include transaction prioritisation for

better, more effectual governance. Transaction prioritisation prioritises overall welfare of public over interests of particular block chain nodes like larger transaction fees, so it contributes to the creation of better world in digital and physical meanings. These disadvantages in the existing work motivate us to carry out this research work. The proposed VONN-FPORC-TP-SC method provides transaction prioritisation in smart city.

The manuscript dwells deep into the comparison of the proposed mechanism with already functional mechanisms in the literature review section. It was found that the consistency and efficiency of the proposed methodology were better than already functional methods in the respective domain. Section 3 provides a clear overview on the designing and mechanising process for our proposed work. Section 4 finds its importance in experimental result and data analysis which in turn relates the proposed method with the practicality of its implementation.

Major contributions of this manuscript are abridged below:

In this manuscript, VONN-FPORC-TP-SC is proposed. Fair proof-of-reputation consensus for blockchain that supports transaction prioritisation is intended to improve smart city administration efficiency, particularly when dealing with crises. Transaction prioritisation is used to record priority transactions so that they may be responded to quickly and without delay. To increase trustworthiness, efficacy of leader election process developed Variational Onsager Neural Networks. For accomplishing trade-off among block production cost, system efficacy a Weighted Byzantine Fault Tolerance consensus process for block formation depend on existence of priority transactions in network is presented. To encourage blockchain nodes to provide truthful feedback on leader's efforts, it proposed a peer-prediction-based feedback collection.

2 Literature survey

Numerous research works presented in literatures depend on transaction prioritisation for smart cities; few of them were reviewed here:

In 2022, Sanghami et al. [20] have presented a ML-improved blockchain consensus by TP-SC. In this paper, the future smart cities fully utilise blockchain technology in domains like data safety, supply chain management, domination, data and energy management, urban management, transportation, and environmental monitoring, including emergency events. It uses a machine learning (ML) algorithm in the consensus protocol to attain effective leader election, to create new dynamic block creation process. Additionally, peer-forecast-based verification mechanism was suggested to guarantee followers 'honest evaluation of leaders' generated blocks. It provides high accuracy and low robustness, while our method is better in both the segments.

In 2022, Uchani Gutierrez and Xu [21] have presented a blockchain with smart contracts to secure property transactions in smart cities. Here, it suggests a strategy to make acquisition, sale of real estate further equal, fair, rather being depending just on amount of money. Smart house is able to classify its present owner by acting as IoT badge, after subject's identification validated, it provided full access to each

services, or blocked and/or reported to authorities. Utilize smart contracts in blockchain to transfer ownership of smart home, which comprises inputs from individuals interested in obtaining an exact house, as outputs from the person who picked the system depend on the Smart City government's previously defined specifications. It provides high efficiency and low promptness index which is not desirable and thus needs future improvement.

In 2021, Chiu and Meng [22] have presented an Edge TC-a PBFT blockchain-dependent ETC system for smart cities. Unlike most other blockchain-dependent ETC platforms utilise PoW or PoS, system employs PBFT for quicker performance. It compares system performance of Ethereum-dependent with Hyperledger-dependent ETC in assessment. The outcomes show that when chain gets lengthy, the Ethereum-based system suffers from inefficiency, but the Hyperledger-dependent ETC maintain consistent time consumption through transactions. It provides high trustworthiness and low accuracy.

In 2023, Nayyer et al. [7] have presented novel framework for fraud detection in bitcoin transactions through ensemble stacking method in smart cities. For data balancing, the suggested model employs ADASYN-TL (Adaptive synthetic + Tomek link) balancing approach. Hyperparameter tuning is accomplished by the use of random search, grid search, and Bayesian optimisation. The hyperparameters have important influence on the method's performance. It employed a stacking model that included DT, NB, K-NN, and RF for classification. SHapley Additive explanation was employed to analyse stacking model's forecasts. It provides high promptness index and low efficiency.

In 2022, Saini et al. [3] have presented a LSP: lightweight smart-contract-dependent transaction prioritisation system for smart medical care. It presents logical stateless transaction methods for various system entities with differing levels of confidence. Finally, method depending on private Ethereum beats the previous benchmark method regarding utility in medical care scenario and computational cost by employing a simple prioritising mechanism. The collected findings show that the suggested approach is feasible in a real-time smart healthcare system. It provides high accuracy and low robustness.

In 2022, Deveci et al. [16] have presented decision support system for evaluating with prioritising maintainable urban transportation in metaverse. Here, it suggests hybrid decision-making framework for prioritising maintainable public transit in Metaverse in setting of q-rung orthopair fuzzy set. To aggregate the qROF information, first q-rung orthopair fuzzy generalised Dombi weighted aggregation operators, features were designed. Second, to determine objective and subjective weights of criteria, q-ROF information-dependent technique depended on removal effects of conditions, and stepwise weight assessment ratio analysis method was provided. It provides high promptness index and low efficiency.

In 2023, Tripathi et al. [23] have presented a new blockchain and IoT-dependent food traceability system for smart cities. A new BIOT-dependent layered structure based on EOSIO was suggested in this study for effective food traceability. Here, determines appropriate traceability units to improve transparency, traceability before defining and implementing layered architecture on the Ethereum with EOSIO blockchain platforms. The suggested EOSIO-based model's performance is assessed

using consensus process's practicability, block production rate, throughput, and block confirmation time. It provides high trustworthiness and low accuracy.

In 2022, Wazid et al. [24] have presented Fortifying smart transportation security through public blockchain. This paper suggests PBSCF-ITS which ensures access control and key management between vehicles, between roadside units, and between roadside units and cloud servers. It examine PBSCF-ITS's security to demonstrate its resistance to many forms of potential assaults. Also, the performance of PBSCF-ITS has been compared to that of other relevant competing systems. The results show that PBSCF-ITS outperforms the current ones. Also, a pragmatic research of PBSCF-ITS being done to examine its impact on key network-related performance factors like as the number of mined blocks and transactions per block. It attains higher promptness index and lower robustness.

3 Proposed methodology

Variational Onsager Neural Networks-based Fair proof-of-reputation consensus for blockchain with Transaction Prioritisation for Smart Cities (VONN-FPORC-TP-SC) is depicted. Block diagram of VONN-FPORC-TP-SC transaction prioritisation for smart cities system is shown in Fig. 1. In system modelling, transaction prioritisation, leader election, block creation, and peer-prediction are the four processes of the proposed method. Thus, the detailed description about VONN-FPORC-TP-SC is given below:

The Variational Onsager Neural Network (VONN) is a deep learning framework that combines ideas from variational inference and the Onsager reaction term in statistical physics. It operates by approximating complex probability distributions and efficiently handling uncertainty in neural networks. VONNs utilise a variational

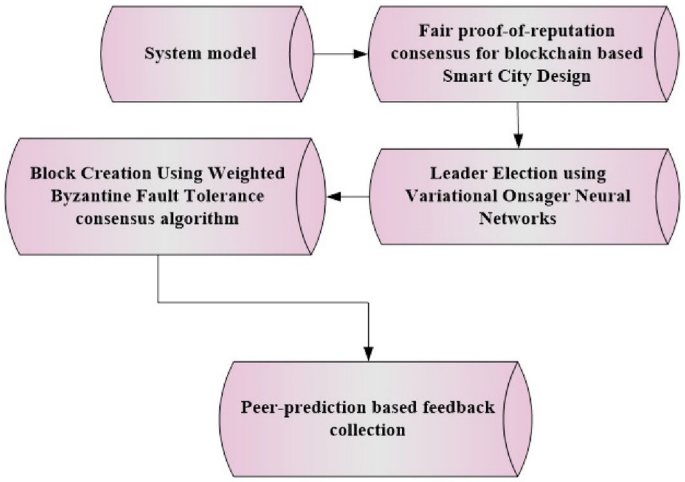


Fig. 1 Block diagram for proposed VONN-FPORC-TP-SC method

approach to estimate posterior distributions, while the Onsager term helps in adjusting predictions by considering prior correlations. This results in more accurate and robust models, particularly in scenarios with noisy or incomplete data. VONNs find applications in fields like signal processing, optimisation problems, and statistical mechanics where accurate probabilistic modelling is essential.

Fair Proof-of-Reputation (PoR) consensus is a blockchain consensus mechanism that ranks and selects validators based on their reputation scores, derived from their behaviour and contributions within the network. Unlike Proof-of-Work (PoW) or Proof-of-Stake (PoS), PoR emphasises long-term trust and reliability, rewarding participants with a positive reputation, while penalising malicious or untrustworthy nodes. This method enhances network security and efficiency by minimising computational waste and incentivizing honest participation. PoR is particularly suitable for decentralised networks, supply chain management, and IoT-based systems where trust and transparency are critical.

3.1 System model

A blockchain-based smart city may be put to many different applications. To integrate, a blockchain network was employed. Transaction prioritisation, or ranking transactions depend on level of urgency, is essential for blockchain network to run smoothly and efficiently. In the absence of transaction prioritisation, this traffic is managed using the standard blockchain approach. Transactions will be validated by the network depending on transaction costs; otherwise, arrival time is determined by the inducement mechanism used. In rare circumstances, this might result in potential injury. Higher priority transaction, like an emergency report, may have to wait for long period its cost is smaller if comes immediately afterwards producing block. Blockchain scheme uses transaction fees incentives for blockchain nodes, a transaction with a greater charge may be registered first.

3.1.1 Transaction prioritisation

This paper aims to prioritise transactions according to their level of urgency by introducing transaction prioritisation to blockchain network [25]. This will ensure transactions with a high level of urgency are handled right away and that the necessary activities are taken relevant party without some delay. Setting transaction priorities guarantee blockchain network's effectiveness and seamless operation. It has assumed that the government provides information about which transactions fall into the categories of high and low priority transactions. Formerly broadcasting the transactions to blockchain network, clients will tag the transactions based on this information. Here, it assumes that the clients will either be truthful or face some sort of punishment. Priority transactions include those involving information that needs to be responded to right away, like maximising traffic lights for emergency vehicles, reporting accidents, detecting water leakage pipes, managing waste overflow. Normal transactions include those that contain generic or routine information, like managing street lights, receiving notifications about road conditions, and receiving

updates from multiple sensors. A regular transaction in blockchain network typically has to wait, but there is priority transaction in pool, transaction is noted right away. Based on this, in the previously mentioned example, traffic light optimisation transactions will be recorded in the network before any other transactions, allowing the emergency vehicle to pass through with ease during heavy traffic and cutting down on emergency vehicle's travel time much as possible. It will assist lowering the dangers to patients' lives and emergency vehicle accidents. The majority of blockchain nodes in the current networks are driven primarily by financial rewards for mining, recording transactions; as a result, prioritise recording transactions by large fees, like those made by Bitcoin miners. The transaction prioritisation mechanism, on the other hand, prioritises transactions according to their level of urgency without giving fees priority, with the overall welfare of the public in mind. As a consequence, implementing transaction prioritisation in current blockchain networks or adding to them becomes difficult since nodes that are motivated by interest may not really carry out transaction prioritisation and instead concentrate on mining only high-fee transactions.

3.2 Blockchain-dependent smart city design

To address difficulty, it will emphasise on implementing consortium blockchain network for smart city applications by a new built FPoR consensus for blockchain to accomplish above-mentioned feature of transaction prioritisation. Because network is permissioned, only nodes accepted with authorised by management body able to validate and record transactions in the blockchain network.

3.2.1 Fair proof-of-reputation consensus for blockchain based smart city design

FPoR consensus for blockchain [26] is discussed. FPoR consensus for blockchain is used to advantage smart city management efficacy, specifically handling emergencies. This system has an effective leader node and several follower nodes. To balance safety, performance, centralisation, scalability in permission less consensus, it introduces FPoR-dependent consensus that make use of collateral, committee-dependent consensus, reputation-dependent node selection, Practical Byzantine Fault Tolerance (PBFT) and incentive mechanisms by reward, penalisation. This system design assumes that each nodes in network are synchronised, making it easier for followers to check leader's work in real-time. Citizens may access any information noted permissioned blockchain via blockchain client interface, assuring transparency, the accessibility of accurate information for use. There may be malicious nodes in permissionless blockchain [27]. Because consensus nodes are chosen at random, a consensus committee comprising many nodes rather than single leader node is chosen through all consensus round to carry out consensus in FPoR. A consensus group committee composed of randomly selected consensus nodes from candidate consensus pool is in charge of block proposal, authentication at each round. To encourage fairness and contribute to blockchain system, consensus nodes in the consensus group are chosen at random depending on reputation in FPoR which means that

each consensus nodes, regardless of reputation, have an equivalent opportunity to participate consensus process. Probability of consensus node is given in Eq. 1,

$$g(j) = \frac{\beta * Cr_K(j) + \gamma * Cy_K(j)}{\sum Cr_K(j) + \sum Cy_K(j)} \tag{1}$$

where $g(j)$ signifies probability, $\beta\&\gamma$ denotes nodes, Cr_K represents the current reputation, and Cy_K represents the cumulative reputation. As consensus nodes are chosen at random, a consensus committee of numerous nodes rather than single leader node is chosen through all consensus round to carry out consensus in FPoR. The leader node records transactions into blocks according to priority, though following nodes check leader's activity. Furthermore, because nodes' rewards or penalties are proportional to their functioning quality, may be confident that system is operating in effectual, honest manner. Average of cumulative reputation is given in Eq. 2,

$$C = \frac{1}{M}\sum_{j=1}^{M}(Cr_K(j)) \geq \frac{1}{m}\sum_{l=1}^{m}(Cr_K(l)) \tag{2}$$

where C represents the average of cumulative reputation, M represents number of nodes in the consensus group, and m represents number of nodes in candidate consensus nodes pool. Collateral is also used in FPoR to avoid sabotage, other bad behaviours through the consensus process. To become candidate consensus node and receive initial reputation value, a participant node must stake token as collateral. Then, all potential consensus nodes are added to a pool of candidate consensus nodes. Average of present reputation is given in Eq. 3,

$$R = \frac{1}{M}\sum_{j=1}^{M}(Cy_K(j)) \geq \frac{1}{m}\sum_{l=1}^{m}(Cy_K(l)) \tag{3}$$

where R represents the current reputation, j &l represents the constant values. To ensure fairness, no member node produce vast majority blocks. In FPoR, same node in the consensus group should not be chosen to process two consecutive blocks. Malicious nodes may collect reputation and raise their chances of being picked as consensus nodes, commit large fraud. To prevent potentially harmful behaviour, total collateral of the consensus group is limited. Total collateral consensus group is given in Eq. 4,

$$T_c = \sum_{j=1}^{M}(collai(j)) \geq \sum_{l=1}^{m}(Wz_{\text{value}}(l)) \tag{4}$$

where T_c represents the total collateral, $collai(j)$ represents the collateral constant, W represents the candidate block, and $z_{\text{value}}(l)$ represents the transaction in candidate block. The existence of fewer nodes for validating transactions than public blockchain improves scalability of used permissioned blockchain, making it appropriate to solving everyday challenges in smart city much more efficiently and quickly. In general, blockchain network adds security layer to vital documents, and these are

mainly vulnerable to corruption, so increasing integrity of smart city administration. The smart city section on right comprises some smart city applications enabled by blockchain network. For good, efficient governance, left box denotes consortium blockchain network, which includes leader, several followers. Thus, the smart city has been designed.

3.3 Consensus mechanism design for transaction-prioritised blockchain

A new consensus mechanism is designed to allow execution of the proposed transaction priority feature for consortium blockchain for smart cities as depicted in Fig. 2. The following section provides an overview of the entire procedure.

3.3.1 Overall procedures of consensus algorithm

Four important steps make up the consensus mechanism that is utilised to accurately record transactions as they enter blockchain network.

- *Leader Election*: In order to ensure that process of prioritising transactions is carried out in honest, effectual manner without leader engaging some types of malicious actions, choosing reliable and effective leader becomes essential to consensus mechanism. To create novel blocks in network, a leader is first selected from blockchain nodes for predetermined amount of time. Some blockchain nodes will follow during that period. Its purpose is to select leader in fair manner while ensuring the leader is efficient node.

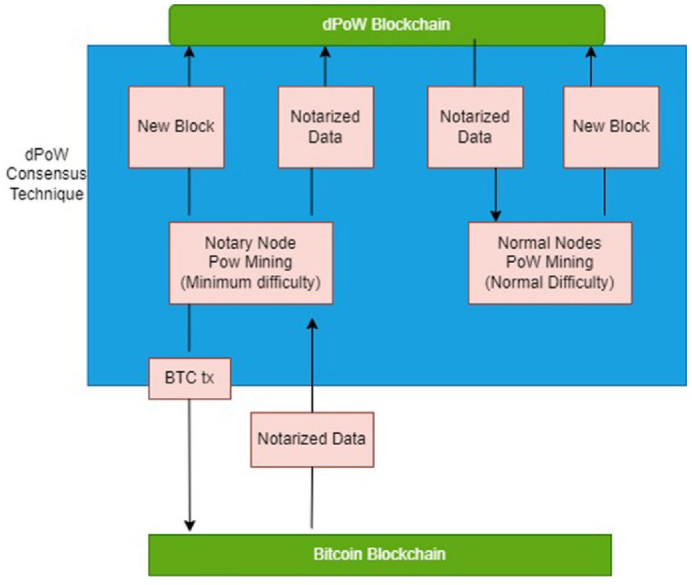


Fig. 2 Selection procedure of consensus algorithm

- *Block creation*: The leader of the consensus algorithm must promptly log every priority transaction that enters the network at that particular moment. Both the priority transactions and the regular transactions that are currently in the pool are recorded instantly. There will be a slight delay before other typical transactions are recorded.
- *Verification*: Next, for verification, the freshly created block is distributed throughout the entire blockchain network. After each block is created, followers review leader's work to see if transaction prioritisation rule is being followed. Peer prediction mechanism is utilised to gather follower feedback so that honesty is taken into account. In order to receive high trustworthiness scores and, as a result, attractive rewards during the incentive distribution step, followers are encouraged to provide honest feedback. The block gets evaluated by the followers and is either accepted, in which case it gets added to the main chain, or rejected. If certain requirements are met, a fresh round of leader elections will also be initiated. To be more specific, the leader records the following block until the maximum number of blocks is reached if review for novel block is satisfactory. The leader is voted out and next leader election process is initiated if review score is unsatisfactory, falling below minimum threshold ($d_{\min}$). Through gossip protocol, every node in blockchain network informed about election its rationale. Also, work is rejected, but leader is providing additional chance to create novel block for error tolerance if it is subpar but falls among range of the minimum ($d_{\min}$), maximum ($d_{\max}$) thresholds.
- *Incentive distribution*: The system's incentive mechanism is based on the leader's feedback regarding the quality of their work and the followers' trustworthiness scores. When incentives are added to the blockchain system by the network's managing body, incentives are dispersed throughout the blockchain network. There is sufficient evidence to accomplish fair incentive distribution because number of blocks created by leaders and the followers' trustworthiness will be noted on the main chain.

3.4 Leader election using Variational Onsager Neural Networks

In this section, the leader election-based blockchain using Variational Onsager Neural Networks (VONN) [28] is discussed. Leader selection becomes an important aspect of the consensus mechanism because choosing trustworthy, effectual leader guarantees that process of prioritising transactions is carried out in honest, effectual way without leader engaging some harmful actions. The leader election process is the first crucial step in the unique VONN for consortium blockchain-dependent smart city, and it consists of dual steps. Finding effectual leader candidates through collecting candidate list, randomly picking leader from that list. Major, Variational Onsager Neural Networks method is used to generate candidate list. To guarantee fairness and avoid DDoS attacks, each truthful node in network has chance to become leader in proof-of-reputation consensus. When leader is chosen, the additional nodes behave as followers for round as given in Eq. 5,

$$x_{j+1} = h_j(Q_j x_j + a_j), \qquad j = 0, ...l \tag{5}$$

where x_{j+1} represents the trustworthiness score, h_j and Q_j represents the efficiency value, x_j represents the vectors, a_j represents the bias vector and $l[NONSPACE]\&j$ represents the variable. Smart contract is triggered after peer-prediction method to collect information about node's honesty score and peers. The blockchain (by timestamps) may be used to acquire a variable l, and hence the value of j. A node functioning as leader is voted out, the information is broadcast to each consortium members, making it available to all nodes in the network. After obtaining this list, randomisation is introduced as the second phase in the leader election process is given in Eq. 6,

$$t(k) = t * [\tilde{t}(k) - \tilde{t}(0)] \tag{6}$$

where $t(k)$ represents the free density $\tilde{t}$ and represents the vote-outs, k represents the efficiency value and $t*$ represents the characteristic scale of $t(k)$. This VONN is executed by current leader of blockchain network to establish candidate list for the succeeding round of leader election in this procedure. Total followers are given in Eq. 7,

$$t(\vartheta, \vartheta^{\varsigma}) = t * \left[\tilde{t}(\vartheta, \vartheta^{\varsigma}) - \tilde{t}(0,0) - \frac{\Phi\tilde{t}}{\Phi\vartheta}; \vartheta\right] \tag{7}$$

where ϑ signifies each follower's honesty while providing comments on the leader's job, ϑ^{ς} represents the degree of the node, Φ represents the total nodes. If current leader is voted out formerly DL method performed for succeeding round of leader election, the candidate node by the greatest trustworthiness score value execute processes to build following candidate list instead. The mathematical calculation of weight matrices is given in Eq. 8,

$$x_{j+1} = h_j(Q_j^x x_j + Q_j^{\infty}\tilde{q} + a_j), \qquad i = 0, ...l \tag{8}$$

where Q_j^x represents the weight matrices, q represents the normalised nodes, a_j represents the bias vector, and x represents the non-negative weights of the nodes. After determining candidate list, current leader else candidate node by higher trustworthiness score (if leader is voted out) uses VONN based on the network's entropy to finish the next leader election process via VONN that cannot be anticipated easily. The vector activation for the nodes given in Eq. 9,

$$y_{j+1} = h_j^y(Q_j^{ty} y_j + a_j^{ty}), \qquad j = 0, 1, ...l - 1 \tag{9}$$

where y_{j+1} represents the vector of activation values, a_j^{ty} represents the bias vector and Q_j^{ty} represents the candidate nodes, and Q represents the function. The entropy based on unconfirmed transaction pool in network. Since the VONN depends on entropy of blockchain network, increase in incoming network traffic will raise level of randomness, causing output to be lesser predictable. Function of $\tilde{Q}$ is given in Eq. 10,

$$Q = \begin{cases} tildeQ + exp(-\epsilon), & \tilde{Q} \geq 0 \\ exp(\tilde{Q} - \epsilon), & \tilde{Q} < 0 \end{cases} \tag{10}$$

where Q represents the function, ϵ represents the positive constant, and $exp(-\epsilon)$ represents experimental constant in the variance. In this system, the VONN function is activated when candidate list is decided by DL, outputs dual random values indicating selected leader, maximum blocks that leader may create. Aforementioned property of entropy-dependent VONN improves the security of blockchain network in terms of resistance to DDoS attacks. The calculation of the critical parameter is given in Eq. 11,

$$\wp(k,q) = \wp * \left[\tilde{\wp}(k,q) - \wp(k,p) - \frac{\Phi\tilde{\wp}}{\wp q}.q\right] \tag{11}$$

where $\wp$ represents the critical parameter, q represents the linear parameter, and $\wp *$ represents the characteristic scale. To identify the candidate nodes, candidate node by highest trustworthiness score value x_{j+1} executes DL. Otherwise, the present leader can keep creating blocks since the bulk of his followers have approved his work. The mathematical model of candidate node is given in Eq. 12,

$$\begin{cases} B_l S(\varpi) = 0, & l = 1, ...m_{PDEs} \\ A_l S(\varpi) = g(\widehat{\varpi}), & l = 1, ...m_{VZs} \end{cases} \tag{12}$$

where A and B represent the operators, S represents the random function generator, ϖ represents the combination of $\widehat{\varpi}$, and g represents the dissimilarity. Current leader's vote-out value is zero; leader is using VONN to find succeeding leader candidate nodes. The current leader's node is given in Eq. 13,

$$fv(Q) = \sum_{l=1}^{m_{\{\mathrm{PED}\}}+m_{\mathrm{VZs}}} fv(L_{ll}) \tag{13}$$

where fv represents the trace of a matrix of random function, L_{ll} represents the matrix block and m_{PDEs} the future parameter. This random function also determines how many blocks the next leader can create. The leader election has been successfully done by using the VONN.

3.5 Block creation using weighted Byzantine fault tolerance consensus algorithm

In this section, block creation using WBFT [29] is discussed. Second stage, leader records transactions from mempool onto major chain using definite criteria. Priority transactions are given greater weight when constructing a block. As a consequence, if even single priority transaction appears, leader must instantly generate a block and record it by other normal transactions in mempool, subsequently broadcast to blockchain network. That rule ensures priority transactions aren't delayed. Management node determines whether node participates in consensus process based on node's threshold. It is given in Eq. 14,

$$GK_j = \frac{Q_j}{Q} \tag{14}$$

where GK_j represents the threshold value, Q_j represents the running weight, and Q represents the base weight. Any time, existence of even single priority transaction in pool results in establishment of a block. Each priority transactions from mempool recorded in block first, surveyed by standard transactions. There is not enough capacity to record each typical transactions, leader will leave few transactions waiting for succeeding block to be created. At finish of all round of consensus, nodes involved in process transmit information input to management node is given in Eq. 15,

$$Q_j = Q_j - U_j \tag{15}$$

where U_j represent severity of punishment. When the amount of transactions entering network is limited, may be few vacant spaces in blocks generated. Normal transactions, on the other hand, may be delayed throughout this procedure. To do this, construct a Weighted Byzantine Fault Tolerance consensus mechanism for leader to use in correctly creating blocks and recording transactions. The activity of the nodes is measured as given in Eq. 16,

$$G_{\text{avg}} = \frac{1}{N} \sum_{j=1}^{N} G_j \tag{16}$$

where G_{avg} represents the average consensus completion time, N signifies number of nodes presented in system, and G_j denotes consensus completion time of *jth* node. By running logs on chain, management node may physically, automatically validate feedback information. The weight updating formula is given in Eq. 17,

$$Q_j = Q_j + 1 \tag{17}$$

On packaging priority transactions, there is a trade-off between block space utilisation and system efficiency. After completing a block, it is broadcast to the network so that the leader's work may be reviewed by the followers. Before creating a new block, the leader must wait for input on that block from the network's follower. Number of consensus nodes in system falls below a certain threshold; the management system will alert you. When replay state is reached, active and primary node relay response to sender node. The protocol specifies maximum number of consensus communications following change given in Eq. 18,

$$B = M \times (M - 1) \tag{18}$$

where B represents the block creation, and M signifies number of nodes in system. The consensus mechanism's block generation time is weighted, depending on whether some priority transactions else enough routine transactions. If transaction is prioritised, block containing produced immediately. The block creation has been done.

3.6 Peer-prediction-dependent feedback collection

Afterwards producing a block, leader broadcasts it to network for verification. Followers must evaluate leader's efforts and give truthful comments. Because certain follower nodes may turn malevolent in order to disrupt smart city governance, peer-prediction technique is utilised to assure authenticity of follower feedback. Because honest input from followers is vital, incentives depend on honesty scores offered to incentivize truthful followers. To safeguard followers' security, feedback from followers is not directly tied to leader's work, but is inferred from gathered forecasts for additional peers. Depending on decision, leader is either voted out else continues to make following block if it has yet to reach the goal of making most blocks. The peer-prediction mechanism, dual smart contracts are employed as execution technique to gather followers' prior, posterior beliefs. At conclusion of every day, prizes entered by smart city governors incentivize leader, followers who engaged in whole consensus process. The incentives for followers proportionate to level of honesty. The incentives for leader mostly determined by number of blocks added to main chain, also comprise transaction fees connected by routine transactions.

3.7 Security analysis

Major benefit of any blockchain network is the potential of safety, anonymity owing to decentralised structure. Blockchain increases secrecy and offers trustworthy environment in which diverse parties may collaborate. Evaluating the security performance of the proposed FPoR consensus for blockchain, it analyses numerous classic blockchain security assaults, like majority attacks, replay attacks, DDoS attacks, and empty block attacks.

3.7.1 Majority attack

While common assault, i.e. the 51% attack, is comparatively challenge to initiate, it will have serious consequences if occurs on blockchain network. Common assault might occur in network as well if blockchain node in network colludes by other nodes, achieves more than 50% control over entire network and after has authority to undermine correct functioning of blockchain-dependent smart city. It will render blockchain network incompetent. Construct the proposed blockchain network in way that attack is prevented by three factors listed below:

- The blockchain network is permissioned, which means that specific nodes accepted by management organisation promoting over-all welfare are permitted to participate in network.
- The follower reports are gathered via peer-prediction approach; it is not advantageous for nodes to collude by one another.
- Because of truthful outcomes obtained through a peer prediction-dependent mechanism, evidently honest, effectual blockchain node attempts to slack off an

else being maliciously after being selected as is leader, blockchain node is voted out directly and and permanently and noted on blockchain, resulting in reduced incentives, being lower possibility of being selected as leader in the future.

3.7.2 DDoS attack

DDoS assaults are widespread on the blockchain network, and they target victim server to launch attack on network through delivering massive network traffic from numerous distributed sources, thereby shutting down victim server. While the blockchain network is decentralised, the leader node in a blockchain-based smart city application might apparently be goal of a DDoS assault. This blockchain network addresses issue via incorporating randomisation into the process of selecting leaders. In detail, leader is chosen at random from a candidates comprised of n nodes, making some pre-deliberate DDoS assault on leader (yet to elected) unbearable. Also, there appears to additional element of susceptibility for DDoS attack in the system as a result of design different blocks permitted to be created leader for efficacy deliberation. It still creates at random maximum blocks a leader can record, amount is only known to other truthful candidates on list. As a result, some hostile actor attempting to attack leader will be unaware of maximum amount of blocks leader may record. It implies every block created by leader at any given time may be leader's last block, therefore assaulting present leader without knowing maximum blocks it make pointless.

3.7.3 Replay attack

Replay attacks are regards among most urbane assaults against the blockchain network. Because of this assault, a blockchain network may undergo protocol modifications or upgrades well-known as hard forks, resulting in a split in the blockchain network, with one side functioning with knowledge of a prior protocol and the other working on a novel protocol. As a result, malevolent nodes may abuse this vulnerability further in order to increase their revenue. This problem is avoided in blockchain-based smart city scenario because we utilise permissioned blockchain, each nodes in network can join only through certification of single management organisation that emphases on welfare society. As a result, protocol change occurs, it is reflected through each nodes supporting object. There are some incorrect transactions or errors; new followers or people with network access can correct the issue by mentioning it.

3.7.4 Empty block attack

Empty block creation is typical function in blockchain network, attack focused on basic process may disrupt blockchain network, rendering it nearly useless. The dynamic block generation strategy protects this blockchain network from this assault by ensuring the leader can't manufacture empty blocks for its individual benefit. If the leader just considers its individual interests and attempts to establish empty blocks for the express purpose of rewarding, the block is rejected, and the leader

votes out directly. The leader can't even get rewards for empty blocks it produces since the rejected block will not be recorded in the main chain; hence, the accompanying prizes will not be received by the leader. Generally, a leader can't act maliciously; when a leader begins acting maliciously, the leader is voted out by follower nodes and loses its benefits. Likewise, follower nodes can't act maliciously; their honesty ratings would badly hurt, affecting their rewards, and their opinions will be ignored. As a result of the above study, it accomplish the blockchain-dependent smart city attains security against the majority of frequent blockchain network threats.

4 Experimental results

Experimental results of indicated procedures are discussed. The VONN-FPORC-TP-SC method is executed using MATLAB R2019b. The data utilised in the experimental result verification were collected through a set of practical implementations whose results were already known or a set of desired results were forehand available. In this experiment, number of blockchain nodes is 1000, and number of peers range from 1 to 999. Maximum number of blocks node may create its maximum honesty score are set to 50 and 10. There is no history of vote-outs, and value of vote-out parameter is 0; there is a history of vote-outs, and value is 1. Several performance measures like Accuracy, Efficiency, Robustness, Trustworthiness, and Promptness index are obtained. Obtained outcomes of proposed VONN-FPORC-TP-SC method are compared with existing methods such ML-BC-TP-SC, BCS-TP-SC, and PBFT-ETC-TP-SC, respectively. Simulation parameters are given in Table 1,

4.1 Performance measures

Accuracy, Efficiency, Robustness, Trustworthiness, Promptness index, and performance metrics are used to describe the performance of proposed strategy.

4.1.1 Accuracy

It is the ratio of count of exact authentication with total number of predictions made for a dataset. It is measured through Eq. 19,

Table 1 Simulation parameters

Parameters	Values
Vote-outs	0
Number of block generated	5
Number of peers	800
Trustworthiness score	1

$$\text{Accuracy} = \frac{\text{Number of correct predictions}}{\text{Total number of predictions}} \tag{19}$$

4.1.2 Efficiency

The capacity to complete a transaction in the most efficient and effective manner feasible, maximising the use of available resources and minimising waste of time, effort, and money, is referred to as transaction efficiency. It entails optimising the processes, systems, and technologies involved in completing a transaction to guarantee that it is accomplished as quickly, accurately, and cost-effectively as possible. It is given in Eq. 20,

$$E = \frac{\text{output}}{\text{input}} \tag{20}$$

4.1.3 Robustness

The capacity of a transaction system to retain its functionality, performance, and integrity in the face of unexpected events or failures is referred to as transaction robustness. It guarantees that transactions are completed accurately and entirely, regardless of any disruptions or mistakes that may occur during transaction processing. It is given in Eq. 21,

$$\text{Robustness} = \frac{\text{availability*integrity*confidentiality}}{\text{vulnerability*risk}} \tag{21}$$

4.1.4 Trustworthiness

The reliability and credibility of a person participating in a transaction, particularly when it comes to honouring their promises and duties, are referred to as trustworthiness in transactions. It signifies that the party can be depended on to consistently and accurately deliver on their obligations, such as giving accurate information, delivering goods or services on time, and preserving confidentiality and ethical behaviour. It is given in Eq. 22,

$$\text{T} = (\text{Credibility} + \text{Reliability} + \text{Intimacy}) \tag{22}$$

4.1.5 Promptness index

The promptness index in transactions is a measurement of how soon a certain transaction is handled or finished. It denotes the speed or efficiency with which a transaction is processed and acts as a measure of how responsive a service provider or system is in satisfying transactional requirements. It is given in Eq. 23,

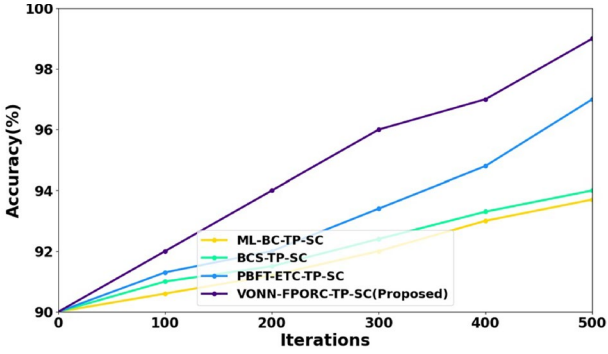


Fig. 3 Accuracy analysis

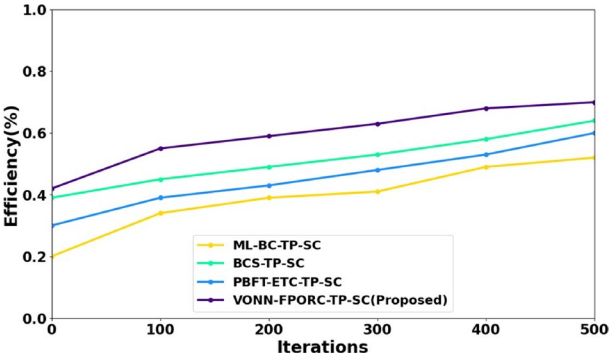


Fig. 4 Efficiency analysis

$$\text{Promptness index} = \frac{\text{total number of prompt deliveries}}{\text{total number of deliveries}} \times 100 \tag{23}$$

4.2 Performance analysis

Figures 3, 4, 5, 6, 7 depict stimulation results of VONN-FPORC-TP-SC proposed method. Then, the proposed VONN-FPORC-TP-SC method is likened to existing methods such as ML-BC-TP-SC, BCS-TP-SC and PBFT-ETC-TP-SC, respectively.

Figure 3 shows accuracy analysis. Here, VONN-FPORC-TP-SC attains 28.86%, 24.47% and 31.79% higher accuracy analysed with existing techniques like ML-BC-TP-SC, BCS-TP-SC, and PBFT-ETC-TP-SC, respectively.

Figure 4 shows efficiency analysis. Here, VONN-FPORC-TP-SC attains 18.25%, 32.27% and 26.89% higher efficiency analysed with existing techniques like ML-BC-TP-SC, BCS-TP-SC, and PBFT-ETC-TP-SC, respectively.

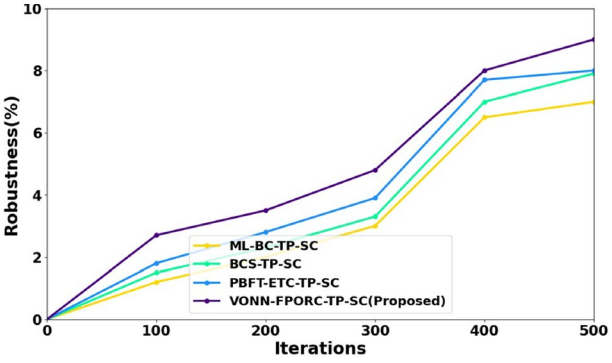


Fig. 5 Robustness analysis

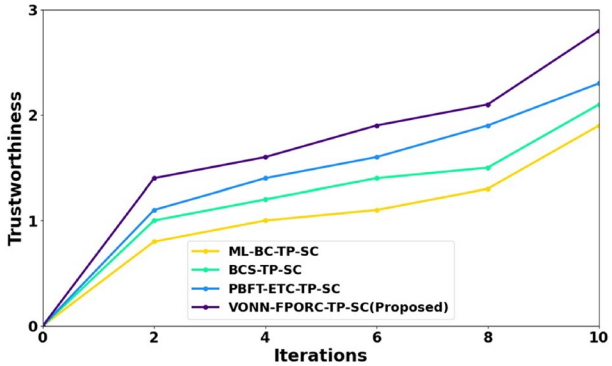


Fig. 6 Trustworthiness analysis

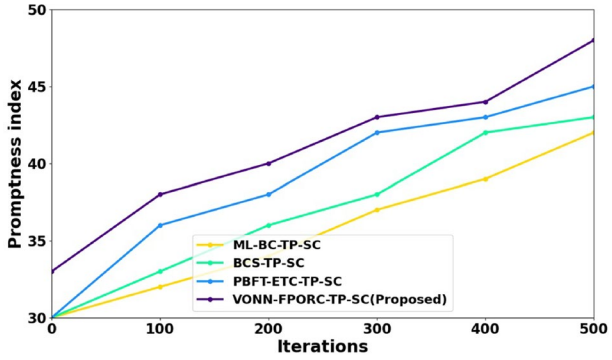


Fig. 7 Promptness index analysis

Figure 5 shows robustness analysis. Here, the proposed VONN-FPORC-TP-SC attains 23.21%, 17.36% and 32.35% higher Robustness analysed with existing techniques like ML-BC-TP-SC, BCS-TP-SC, and PBFT-ETC-TP-SC, respectively.

Figure 6 shows trustworthiness analysis. Here, VONN-FPORC-TP-SC attains 16.29%, 27.38% and 33.45% higher trustworthiness analysed with existing technique like ML-BC-TP-SC, BCS-TP-SC, and PBFT-ETC-TP-SC, respectively.

Figure 7 shows promptness index analysis. Here, VONN-FPORC-TP-SC attains 32.12%, 29.21% and 19.99% higher promptness index analysed with existing technique like ML-BC-TP-SC, BCS-TP-SC, and PBFT-ETC-TP-SC, respectively.

4.3 Discussion

In this work, the VONN-FPORC-TP-SC model for the blockchain consensus with transaction prioritisation is used in smart cities. The transaction prioritisation function was included to aid in the timely recording of transactions containing vital information. For an efficient leader election process, it created a method that uses a Variational Onsager Neural Network with a random function. The convincing simulation outcomes demonstrate accuracy, hence the efficiency of applied block generation. VONN additionally proposed a new weighted Byzantine fault tolerance consensus policy. Four node metrics are significant in determining leader candidates in this VONN. Four node metrics are significant in determining leader candidates in this VONN. They are number of peers, honesty score, number of produced blocks, and voting history. After the selection of leader candidates, adapted true random number generator function is launched; it randomly choose leader from list and offer maximum amount of blocks that leader may record period. Blockchain network is simulated in peer-prediction method to examine the relevance of honesty value and influence of additional factors on honesty value. Blockchain nodes are classed as truthful or malevolent based on their trustworthiness levels. Here, the peers approach 480, and forecast becomes 1. The peers reach 480, overall value of node exceeds threshold value, and blockchain node is selected as leader candidate. When promptness index $1 - \Phi$ is modified from 300 to 400, the Φ value remains constant 43.5. Likewise, Φ is modified, promptness index remains constant at 45. Because honesty value is directly proportional to promptness index $1 - \mu$, an increase promptness index leads to an increase in honesty score. Proposed method analysed with existing techniques like ML-BC-TP-SC, BCS-TP-SC, and PBFT-ETC-TP-SC, respectively. When analysed with existing techniques, accuracy of proposed method is 99.5%. The efficiency more than 96% comparing with the existing methods. It concludes that the proposed VONN-FPORC-TP-SC method is better than existing models for TP-SC.

5 Conclusion

In this manuscript, VONN-FPORC-TP-SC is successfully implemented. This method created a Fair proof-of-reputation for smart city design and VONN for leader election. The influence of several characteristics on the trustworthiness value

was explored using peer prediction-dependent approach meant to inspire truthful input from followers for evaluation of the leader's performance. Also, build-up trustworthiness value over time was investigated in order to distinguish the behaviour of honest and malevolent nodes. The performance of the proposed VONN-FPORC-TP-SC method attains 32.12%, 29.21% and 19.99% higher promptness index and 16.29%, 27.38% and 33.45% higher trustworthiness when analysed to the existing methods such as ML-BC-TP-SC, BCS-TP-SC, and PBFT-ETC-TP-SC, respectively.

Author contributions Chandra Prakash Singh contributed to Methodology, validation, data curation, writing—original draft. Rohita Yamaganti contributed to project administration. Lokendra Singh Umrao contributed to conceptualisation, formal analysis, supervision, writing—reviewing, and editing. All authors read and approved the final manuscript.

Funding This research received no external funding.

Data availability All data generated or analysed during this study are included in this article.

Declarations

Conflict of interest The authors have declared no conflict of interest in this work.

Ethics approval and consent to participate The submitted work is original, and the manuscript has not been submitted to another journal for simultaneous consideration.

Consent for publication The authors declare that they consent to publish the article.

References

1. Malik V, Mittal R, Mavaluru D, Narapureddy BR, Goyal SB, Martin RJ, Srinivasan K, Mittal A (2023) Building a secure platform for digital governance interoperability and data exchange using blockchain and deep learning-based frameworks. IEEE Access 11:70110–70131. https://doi.org/10.1109/ACCESS.2023.3293529
2. Cali U, Deveci M, Saha SS, Halden U, Smarandache F (2022) Prioritizing energy blockchain use cases using type-2 neutrosophic number-based edas. IEEE Access 10:34260–34276. https://doi.org/10.1109/ACCESS.2022.3162190
3. Saini A, Wijaya D, Kaur N, Xiang Y, Gao L (2022) Lsp: Lightweight smart-contract-based transaction prioritization scheme for smart healthcare. IEEE Int Things J 9(15):14005–14017. https://doi.org/10.1109/JIOT.2022.3145406
4. Yaraghi AS, Bagherzadeh M, Kahani N, Briand LC (2023) Scalable and accurate test case prioritization in continuous integration contexts. IEEE Trans Softw Eng 49(4):1615–1639. https://doi.org/10.1109/TSE.2022.3184842
5. Chakraborty C, Mishra K, Majhi SK, Bhuyan HK (2023) Intelligent latency-aware tasks prioritization and offloading strategy in distributed fog-cloud of things. IEEE Trans Ind Inform 19(2):2099–2106. https://doi.org/10.1109/TII.2022.3173899
6. Heidary-Dahooie J, Rafiee M, Mohammadi M, Meidute-Kavaliauskiene I (2022) Proposing a new lsgdm framework based on bwm with hesitant fuzzy information for prioritizing blockchain adoption barriers in supply chain. Technol Soc 71:102146. https://doi.org/10.1016/j.techsoc.2022.102146
7. Nayyer N, Javaid N, Akbar M, Aldegheishem A, Alrajeh N, Jamil M (2023) A new framework for fraud detection in bitcoin transactions through ensemble stacking model in smart cities. IEEE Access 11:90916–90938. https://doi.org/10.1109/access.2023.3308298

8. Lopez-Cubillos S, Runting RK, Suárez-Castro AF, Williams BA, Armenteras D, Ochoa-Quintero JM, McDonald-Madden E (2022) Spatial prioritization to achieve the triple bottom line in Payment for ecosystem services design. Ecosyst Serv 55:101424. https://doi.org/10.1016/j.ecoser.2022.101424
9. Li N, Haralambides H, Sheng H, Jin Z (2022) A new vocation queuing model to optimize truck appointments and yard handling-equipment use in dual transactions systems of container terminals. Comput Ind Eng 169:108216. https://doi.org/10.1016/j.cie.2022.108216
10. Mora Cortez R, Hidalgo P (2022) Prioritizing b2b marketing capabilities: crossvergence in advanced and emerging economies. Ind Marketing Manag 105:422–438. https://doi.org/10.1016/j.indmarman.2022.07.002
11. Pomeroy-Stevens A, Goldman B, Grattan K (2022) Participatory Systems mapping for municipal prioritization and planning. J Urb Health 99(4):738–748. https://doi.org/10.1007/s11524-022-00654-2
12. Sangaiah AK, Javadpour A, Ja'fari F, Pinto P, Ahmadi H, Zhang W (2022) Cl-mlsp:the design of a detection mechanism for sinkhole attacks in smart cities. Microprocess Microsyst 90:104504. https://doi.org/10.1016/j.micpro.2022.104504
13. Davlyatov S (2023) Smart-city ecosystem using block-chain technology. In: 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), pp. 1077–1080. doi:/10.1109/ICACITE57410.2023.10183248
14. Siddiqui S, Hameed S, Shah SA, Khan AK, Aneiba A (2023) Smart contract-based security architecture for collaborative services in municipal smart cities. J Syst Archit 135:102802. https://doi.org/10.1016/j.sysarc.2022.102802
15. Dwivedi YK, Hughes L, Kar AK, Baabdullah AM, Grover P, Abbas R, Andreini D, Abumoghli I et al (2022) Climate change and COP26: are digital technologies and information management part of the problem or the solution? An editorial reflection and call to action. Int J Inform Manag 63:102456. https://doi.org/10.1016/j.ijinfomgt.2021.102456
16. Deveci M, Mishra AR, Gokasar I, Rani P, Pamucar D, ozcan E (2023) A decision support system for assessing and prioritizing sustainable urban transportation in metaverse. IEEE Trans Fuzzy Syst 31(2):475–484. https://doi.org/10.1109/TFUZZ.2022.3190613
17. Dahmane WM, Ouchani S, Bouarfa H (2022) Guaranteeing information integrity and access control in smart cities through blockchain. J Ambient Intell Humaniz Comput 14(9):11419–11428. https://doi.org/10.1007/s12652-022-03718-y
18. Alam T (2021) Blockchain cities: the futuristic cities driven by blockchain, big data and internet of things. GeoJournal 87(6):5383–5412. https://doi.org/10.1007/s10708-021-10508-0
19. Javaid M, Haleem A, Pratap Singh R, Khan S, Suman R (2021) Blockchain technology applications for industry 4.0: a literature-based review. Blockchain Res Appl 2(4):100027. https://doi.org/10.1016/j.bcra.2021.100027
20. Sanghami SV, Lee JJ, Hu Q (2023) Machine-learning-enhanced blockchain consensus with transaction prioritization for smart cities. IEEE Internet Things J 10(8):6661–6672. https://doi.org/10.1109/JIOT.2022.3175208
21. Uchani Gutierrez OC, Xu G (2023) Blockchain and smart contracts to secure property transactions in smart cities. Appl Sci. https://doi.org/10.3390/app13010066
22. Chiu W-Y, Meng W (2021) EdgeTC - a PBFT blockchain-based ETC scheme for smart cities. Peer Peer Netw Appl 14(5):2874–2886. https://doi.org/10.1007/s12083-021-01119-0
23. Tripathi AK, Krishnan KA, Pandey AC (2023) A novel Blockchain and internet of things-based food traceability system for smart cities. Wirel Pers Commun 129(3):2157–2180. https://doi.org/10.1007/s11277-023-10230-9
24. Wazid M, Bera B, Das AK, Mohanty SP, Jo M (2022) Fortifying smart transportation security through public blockchain. IEEE Internet Things J 9(17):16532–16545. https://doi.org/10.1109/JIOT.2022.3150842
25. Umrao LS, Singh RS (2015) Fault-tolerant routing over shortest node-disjoint paths in hypercubes. Int J Parallel Emerg Distrib Syst 31(3):294–304. https://doi.org/10.1080/17445760.2015.1057587
26. Zhang T, Huang Z (2023) Fpor:fair proof-of-reputation consensus for blockchain. ICT Express 9(1):45–50. https://doi.org/10.1016/j.icte.2022.11.007
27. Umrao LS, Patel SC, Kumar S (2022) Blockchain-based reliable framework for land registration information system. Int J Technol Diffus 13(1):1–16. https://doi.org/10.4018/ijtd.300743

28. Huang S, He Z, Chem B, Reina C (2022) Variational onsager neural networks (vonns):a thermodynamics-based variational learning strategy for non-equilibrium pdes. J Mech Phys Solid 163:104856. https://doi.org/10.1016/j.jmps.2022.104856
29. Qin H, Cheng Y, Ma X, Li F, Abawajy J (2022) Weighted byzantine fault tolerance consensus algorithm for enhancing consortium blockchain efficiency and security. J King Saud Univ Comput Inform Sci 34(10):8370–8379. https://doi.org/10.1016/j.jksuci.2022.08.017

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.

Authors and Affiliations

Chandra Prakash Singh[1] · Rohita Yamaganti[1] · Lokendra Singh Umrao[2]

✉ Lokendra Singh Umrao
lokendra.rs.cse12@iitbhu.ac.in

Chandra Prakash Singh
cp.singh1984@gmail.com

Rohita Yamaganti
rohita.yamaganti@gmail.com

[1] Department of Computer Science and Engineering, P. K. University, Karera, Shivpuri, M.P. 473665, India

[2] Department of Computer Science and Engineering, Dr. Rammanohar Lohia Avadh University, IET Campus, Ayodhya, U.P. 224001, India

Peer-to-Peer Networking and Applications (2026) 19:3
https://doi.org/10.1007/s12083-025-02168-5

RESEARCH

A privacy-preserving and secure framework using blockchain-based quantum-inspired complex convolutional neural network for IoT-driven smart cities

Chandra Prakash Singh[1] · Rohita Yamaganti[1] · Lokendra Singh Umrao[2]

Received: 29 March 2025 / Accepted: 3 November 2025
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2025

Abstract

The developments of Internet of Things (IoT), smart cities have become majority of urbanization. IoT networks use the Internet as an open channel to enable distributed smart devices to collect and process data within the architecture of smart cities. In this paper, a privacy-preserving and secure framework using a blockchain-based quantum-inspired complex convolutional neural network for IoT-driven smart cities (PSF-BCH-QICCN-IoT) is proposed. Initially, the dataset was taken from the BoT-IoT dataset. The data collected are fed to blockchain-based Proof-of-Monitoring (PoM) for privacy-preserving and secure framework. Then feature mapping and feature selection are formed using the Hunger Game Search Optimization Algorithm (HGSOA). After that, QICCN is utilized to classify anomalies such as Denial-of-Service, Distributed DoS, Normal, Reconnaissance, and Theft. Generally, QICCN does not show some optimization adaption techniques to determine the optimum parameter to offer accurate detection. Firebug Swarm Optimization (FSO) process is proposed to enhance QICCN and classify the anomaly precisely. The performance of proposed technique is analyzed using performance metrics such as accuracy, specificity, recall, precision, F1-score, false alarm rate. The proposed (PSF-BCH-QICCN-IoT) method achieves accuracies of $\mathbf{88.67}\%$, $\mathbf{87.23}\%$, and $\mathbf{90.45}\%$ on the respective datasets, which correspond to improvements of $\mathbf{23.33}\%$, $\mathbf{21.45}\%$, and $\mathbf{31.35}\%$ over the baseline accuracies of $\mathbf{71.87}\%$, $\mathbf{71.82}\%$, and $\mathbf{68.84}\%$; $\mathbf{34.15}\%$, $\mathbf{32.26}\%$ and $\mathbf{19.95}\%$ higher precision; $\mathbf{25.55}\%$, $\mathbf{27.35}\%$ and $\mathbf{22.15}\%$ higher recall analyzed to the existing methods, like developing effectual feature engineering along machine learning technique for identifying IoT-botnet cyber-attacks (DMLP-IoT-BAD), feature engineering depend performance analysis of ML-DL processes for Botnet attack identification in IoMT (SVM–IoT-BAD) and intrusion identification scheme for IoT botnet attacks utilizing deep learning (DNN-IoT-BAD), respectively.

Keywords Blockchain technology · Smart cities · Firebug swarm optimization · Hunger game search optimization algorithm · Quantum-inspired complex convolutional neural network · Proof-of-monitoring

1 Introduction

By 2050, almost 70% of the world's population is projected to live in urban areas [1]. Several nations have proposed the concept of "smart cities" in an attempt to manage urbanization more effectively. Generally speaking, a "smart city" is one that uses technology-based methods, such as IoT, big data exploration, cyber-physical schemes, real-time control, improves and then gives its residents a pleasant living. It is widely acknowledged that IoT is crucial in allowing technology to unite completely dispersed sensors, smart devices to gather, analyze data via the Internet, an open channel, for the infrastructure of smart

Chandra Prakash Singh, Rohita Yamaganti, and Lokendra Singh Umrao contributed equally to this work.

✉ Lokendra Singh Umrao
lsucs@mmmut.ac.in

Chandra Prakash Singh
cp.singh@srgi.ac.in

Rohita Yamaganti
rohita.y@sreenidhi.edu.in

[1] Department of Computer Science & Engineering, P.K. University, Karera, Shivpuri 473665, M.P., India

[2] Department of Computer Science & Engineering, Madan Mohan Malaviya University of Technology, Deoria Road, Gorakhpur 273010, U.P., India

Published online: 11 November 2025

cities [2–4]. Smart city applications, which cover a wide range of industries such as medical care, energy management, transportation, water, and irrigation management, are mostly dependent on the effective use of data produced by sensors and devices. Numerous sensors are connected to the Internet in smart cities [5, 6]. Security and privacy problems follow accordingly from this. First, interconnectivity of IoT sensors raises security concerns and presents a number of potential dangers to IoT devices in smart cities. Physical and/or cyber-attacks are two main types of smart city attacks. When an adversary physically attacks an IoT sensor, they can simply alter or tamper with the sensors and devices that are used for communication. In cyber-attacks, the adversary tries to install malicious software or harmful software in the components of the smart city [7, 8]. This assault comprises permanent DoS, malicious code injection, fake node injection. These attacks include backdoor, ransomware, eavesdropping, DDoS, DoS. The second privacy concern is the compromise of private data through inference, data poisoning attacks. A hacker attempting to modify the data from a smart object by adding bogus measurement data is known as a data poisoning or inference attack [9–11]. The consequences of this are negative for machine learning-based intrusion detection and data analytics systems [12, 13]. These assaults have the potential to disrupt regular device connectivity and result in inefficient power use by IoT devices. Therefore, maintaining privacy and security is essential for smart cities and their networks.

Deploying smart devices, sensors that offer ubiquitous experience and prevalent environment is a goal of the Internet of Things. Ensuring secure and private services that are transparent and seamless is the main difficulty in the deployment of IoT. Different IDSs/IPSs that leverage machine learning, advanced statistical methodologies to ensure IoT security [14–17]. However, to address computational needs, the majority of conventional security systems currently in use, however, rely on cloud-based centralized deployment. A further challenge in a centralized setting is that it is multiparty governed and does not have traceability or transparency. Multiparty management and lack of traceability and transparency present additional challenges in a centralized setting [18, 19]. Using a fog computing architecture, in which computational resources are moved, processed close to users or devices, is one possible approach. IoT fog computing offers a number of benefits, including the path to data offloading, decreased communication latency, and increased spectral efficacy. Moreover, edge devices are in charge of collecting and analyzing the data that is obtained fog. Based on their needs, these edge-processed data are aggregated, sent to the cloud network for additional processing and other long-term storage, or sent directly to the contributing IoT devices [20]. However, integration of IoT-fog creates new difficulties for the scalability, verifiability, safety, and privacy of data produced through IoT devices. The underlying technology is made up of several components, including a tamper-resistant ledger, integrity, and immutability. Therefore, implementing blockchain technology in smart cities driven by the IoT improves data safety and privacy. Blockchain technology needs to be thoroughly studied to solve the issues mentioned above with smart cities driven by IoT. It is a distributed technology that is trustworthy and decentralized [21–23]. It enables trust, auditability, immutability, and data transparency of the distributed IoT node. In addition, it can track unaffected historical records without tampering with the ledger. Blockchain technology makes it costly to store large amounts of data; however, it works well to store data hashes in the ledger rather than actual data [24, 25]. This study employs the Inter Planetary File System (IPFS); distributed file system is content-addressable with data saved by excellent reliability and durability, taking into account the limited storage space of all blockchain nodes. Data are copied and stored on the Internet in different IPFS nodes; IPFS does not have a central server. Every file submitted to IPFS is assigned a distinct hash. The real data are kept in IPFS for each transaction in the blockchain-IPFS connection; returned novel hash is uploaded to the block [26]. As a result, a clever Fog-Cloud design that integrates IPFS with Blockchain may be an appropriate deployment framework.

The novelty of this research lies in the integration of a lightweight, yet effective CNN-based model with a privacy-preserving framework specifically designed for resource-constrained IoT smart devices. Unlike existing approaches, which often require large amounts of computational resources or do not take into account privacy concerns, our method achieves high accuracy while maintaining a low processing footprint. The model architecture is optimized to run efficiently on embedded systems, and the privacy mechanism ensures secure data handling, making it highly suitable for real-world deployment in smart IoT environments.

The major contribution of this method is summarized below:

- Propose a dual-level privacy protection scheme. The initial level comprises blockchain, the enhanced PoM method based on smart contracts using network. PoM operates by generating a unique cryptographic hash for each metadata object, which is then recorded on a distributed ledger. This hash not only ensures the integrity of the content, but also serves as a tamper-proof reference. Unlike PoW, PoM does not rely on

computational puzzles; instead, it verifies uniqueness and integrity through deterministic hashing and cross-node consensus on metadata validity. This significantly reduces energy consumption compared to PoW, while still providing strong immutability guarantees through decentralized verification and metadata anchoring. Additionally, PoM incorporates redundancy checks to detect and eliminate duplicate or malicious data submissions. This level authenticates records of IoT data and averts modification of unique data by data poisoning attacks. The second level utilizes HGSOA depend on feature mapping and feature selection that transforms authenticated IoT data into novel encoded format and avoids inference attack data learned from system-depending QICCN.

- Evaluate the capability of the (PSF-BCH-QICCN-IoT) framework to discover numerous cyber attacks on smart city networks.
- A decentralized deployment solution through the integrating blockchain-IPFS is present fog-cloud architecture is suggested. This deployment approach mitigates the limitations of current fog-cloud else stand-alone cloud-based deployments. IPFS was chosen over alternative distributed storage solutions due to its efficient use of decentralized peer-to-peer architecture, low-latency retrieval through distributed hash tables (DHT), built-in versioning, and its ability to prevent data duplication. These features make it particularly suitable for applications where data integrity, scalability, and long-term accessibility are critical.
- The PSF-BCH-QICCN-IoT method is assessed using BoT-IoT dataset; systems' performance is analyzed with some of the latest state-of-the-art peer privacy preservation techniques to determine its efficiency.

The integration of a sophisticated CNN with privacy-preserving strategies designed for resource-constrained IoT environments makes the suggested method unique. Through an architecture tailored to the computational and communication constraints of smart devices, our approach simultaneously optimizes both model accuracy and privacy protection, in contrast to previous works that only concentrate on one of these two areas. Decentralized learning mechanisms and lightweight components are incorporated into the model design to protect data privacy without compromising performance. Our method is especially well suited for deployment in real-world IoT applications, where protecting user data is just as important as achieving high inference accuracy, because of its dual focus on efficiency and security.

2 Literature review

Several study efforts in the literature indicated privacy-preserving with a secure framework utilizing blockchain-dependent ML for IoT-driven smart cities; rare current studies are examined here:

In 2021, Kumar et al. [27] have presented privacy preservation with a secure framework using blockchain-dependent ML for smart cities driven by the IoT. Here, suggested PPSF was based on dual key mechanisms: First, a blockchain module created to safely transfer IoT data was used and a principal component analysis (PCA) method was utilized to give the unprocessed data a novel form in a dual-level privacy system. A Gradient Boosting Anomaly Detector was utilized in the intrusion detection technique to train and assess the proposed dual-level privacy system, which was dependent on the dataset from the dual IoT network dataset: ToN-IoT, BoT-IoT. Additionally, we recommend integrating the Fog-Cloud architecture using IPFS and blockchain to implement the proposed framework. It provides high precision, low accuracy.

In 2021, Kumar et al. [28] have presented a trustworthy secure privacy preservation framework for maintainable smart cities using blockchain and ML. Here, the two-tier privacy suggested that module along with an intrusion detection module. In the trustworthiness module, the blockchain reputation system is based on addresses. The dual-level privacy module transforms data into a novel reduced shape to thwart inference, poisoning attempts by applying PCA and improved Proof-of-Work method dependent on blockchain simultaneously. An optimized gradient tree-boosting technique is implemented in the intrusion detection module. Provides high accuracy and low recall.

In 2021, Kumar R. et al. [29] have presented a privacy-preserving dependence secure framework utilizing blockchain-enabled DL in a cooperative intellectual transport system. In this paper, the proposed architecture uses deep learning modules and blockchain technology to give two levels of security and anonymity. A DL module was constructed that integrates the LSTM-AE method to encode C-ITS data into a novel format, thus protecting against inference attacks. Two datasets, ToN-IoT and CICIDS-2017, that are accessible to the public are used to further validate and test the system. Provides higher accuracy with lower specificity.

In 2021, Kumar et al. [30] have presented a blockchain with DL framework for the privacy-preserved threat intellect in industrial IoT. Here, a novel P2TIF was developed to detect cyber threats in IIoT contexts and protect sensitive data. Initially, a blockchain module that can

be expanded and offers secure IIoT data transport while protecting against data poisoning. Secondly, DL module called deep variational auto encoder (DVAE) that protects against inference attacks by rearranging real data into a secure format. Then, a threat detection system employs the encoded data to identify dangerous patterns in IIoT environments by using a deep-gated recurrent neural network dependent on attention. It provides high precision and high false rate.

In 2023, Ahamad et al. [31] have presented a dual-level blockchain-dependent privacy preservation framework in IoT using the DL architecture supported by the heuristic fusion mechanism. In this work, a novel method for the preservation of privacy based on the IoT, embraced by blockchain technology, is being developed to offer increased security while minimizing the use of resources. Deep learning is the method used to achieve two degrees of data privacy. As a result, encrypted data was sent to the data decryption procedure, where it is processed by the auto-encoder decoder to recreate the original data. It attains higher recall, lower specificity.

In 2022, Hamouda et al. [32] have presented a secure privacy-preserving framework using federated DL allowed by blockchain for industrial IoT. This study suggested that a unique privacy-preserving secure framework (PPSS) with enhanced privacy, verifiability, and transparency was built on the use of FL-allowed by the blockchain. In order to protect client updates' privacy, the initial step utilizes differentially private training of stochastic gradient descent, the second stage utilizes the PoFDL protocol to validate, add novel blocks to blockchain that contain models. Provides higher accuracy, lower precision.

In 2022, Sanghami et al. [33] have presented the ML-enhanced blockchain consensus by transaction prioritization for smart cities. Here, a suggested first-served processing method is applied, which endangering people's lives. As a result, fast block construction and transaction prioritization are required based on information priority. Additionally, since the leader will guarantee transaction priority when creating blocks, it is crucial for the transaction prioritization process to occur in our consortium blockchain in an honest and effective manner that leader rotation and appropriate election procedures are followed. Use ML technique in consensus protocol to achieve effective leader election, create new dynamic block construction mechanism. Provides high recall and low F1-score.

In 2025, Althaf Ali et al. [34] have presented a way to secure the medical data of smart city applications through a collaborative blockchain based on Federated Learning (FL) enabled. Here, utilizing the Zero Knowledge Proof (ZKP) technique, a new scalable blockchain architecture was suggested to guarantee data integrity and secure data transmission. Next, a Blockchain-enabled Federated Learning (BFL) framework is implemented through an ethereum smart contract to handle data safety concerns with IPFS off-chain storage to address data storage costs. To detect intrusions into the HS network, a deep learning architecture is designed utilizing verified data. The latter creates efficient IDS by combining Bi-LSTM with a Deep Sparse Auto Encoder. Provides a high F1-score and low precision.

Although numerous studies have explored security and privacy concerns in IoT systems, many existing solutions focus on isolated aspects. Either enhancing model accuracy or improving data protection, without offering a unified framework suitable for resource-constrained environments. For example, traditional deep learning models require centralized training, posing privacy risks, while some privacy-preserving methods significantly degrade performance or are computationally intensive. Our work addresses this gap by combining a lightweight CNN architecture with privacy-preserving techniques such as blockchain-based federated learning, specifically adapted for IoT devices. This approach directly responds to the challenges of limited computational resources, vulnerability to data leakage, and the need for decentralized learning. Thus, offering a practical and scalable solution for real-world IoT deployments.

Blockchain technology has emerged as a promising solution to address several persistent security and trust challenges in IoT systems [35–37]. The decentralized nature of blockchain eliminates reliance on centralized authorities, which are often single points of failure in traditional IoT architectures. In addition, blockchain ensures data integrity and resistance to tampering through cryptographic hashing and consensus mechanisms, making it particularly suitable for environments with a high risk of data spoofing or unauthorized access. Given the assumptions in our work, namely that IoT devices operate in potentially untrusted, distributed networks and often lack strong built-in security, a blockchain offers a robust, distributed ledger for secure transaction recording, device authentication, and access control. By incorporating blockchain into our proposed framework, we aim to provide a verifiable, scalable, and low overhead security layer that complements our CNN-based privacy-preserving model and addresses the core vulnerabilities found in contemporary IoT deployments.

Security, privacy, and interoperability are some of the issues that the IoT presents that can be resolved by combining blockchain technology with the IoT [4]. For example, by offering a decentralized and impenetrable platform

for data exchange, blockchain technology can improve the security and privacy of IoT networks. Blockchain technology can also open up new revenue streams and business models, such as data sharing between stakeholders. There are many uses for blockchain and IoT integration in a range of sectors, including healthcare and smart cities. Blockchain-based IoT networks have the potential to enable healthcare providers to securely and openly share patient data. By facilitating real-time data exchange between vehicles and infrastructure, blockchain-based IoT networks have the potential to improve the safety and efficiency of smart city systems [38].

Several significant parallels motivate the technological integration of ML, blockchain, and IoT in smart cities. First, data-driven decision making is facilitated by all three technologies. While IoT continuously collects vital data in municipal services, machine learning (ML) analyzes the massive information from IoT devices to optimize urban operations in real-time. Blockchain guarantees these data's security and integrity, facilitating trustworthy decision-making procedures. Decentralization is another similarity; ML gains from decentralized data processing techniques such as FL, which lower latency and improve privacy. IoT networks are also decentralized by nature, with many devices functioning independently. The distributed nature of IoT and ML is well complemented by blockchain, which offers a decentralized, secure architecture that guarantees no single point of control over data. In addition to decentralization and data-driven decision making, common challenges and objectives include scalability and adaptability. Like IoT systems, ML models must be able to handle a growing number of devices and shifting network demands, as well as scale and adjust to changing urban conditions and growing data volumes. Lastly, even though blockchain has scalability issues, especially as IoT transactions increase, sophisticated solutions are being created to improve its performance and scalability.

The comparative analysis among Blockchain + IoT, Blockchain + ML and IoT + ML is given in the following table. Blockchain + IoT is best for trust and traceability in device ecosystems, particularly where data integrity and auditability are critical. Blockchain + ML is ideal for secure, decentralized learning environments where data sharing and model trust need to be verifiable. IoT + ML excels in real-time decision-making and automation, offering edge intelligence for smart environments. Each combination plays a distinct role, and hybrid integration of all three technologies (Blockchain + IoT + ML) is increasingly seen in advanced systems such as autonomous vehicles, smart healthcare and industrial 4.0 settings.

Comparative Analysis: Blockchain + IoT vs. Blockchain + ML vs. IoT + ML

Aspect	Blockchain + IoT	Blockchain + ML	IoT + ML
Purpose	Enhance trust, security, and decentralization in IoT networks.	Secure and audit ML processes, ensure trust in training data, and enable decentralized ML.	Improve real-time decision-making and automation in IoT systems using intelligent data analytics.
Key Strengths	Decentralized data management, Immutable logs for traceability, Enhanced device authentication and data integrity	Tamper-proof data for ML, Model auditability and provenance, Secure data sharing for collaborative learning	Predictive analytics, Real-time data processing, Intelligent automation and pattern detection
Key Limitations	Scalability issues (due to blockchain latency), High energy consumption (especially with PoW), Complexity of integrating with resource-constrained IoT devices	High computational requirements, Blockchain's slow transaction speeds impact ML workflows, Data privacy vs. transparency trade-offs	Data privacy concerns, Requires substantial training data, Edge devices may lack processing power
Architecture Implications	Requires lightweight blockchain protocols, Needs off-chain/on-chain data balance	Integration of blockchain smart contracts with ML pipelines, Often uses decentralized or federated learning	Combines edge computing and cloud analytics, Often needs real-time feedback loops
Security Benefits	Protects against data tampering, Prevents single points of failure	Guarantees data integrity for training, Secure access control for ML models and datasets	Detects anomalies and potential attacks, However model itself can be vulnerable
Example Use Cases	Supply chain monitoring, Smart cities (e.g., utility monitoring), Secure sensor networks	Federated learning across institutions (e.g., healthcare), Verifiable AI decisions (e.g., finance, governance)	Smart homes, Predictive maintenance in industrial IoT, Traffic management and optimization
Real-World Example	IBM's Food Trust for supply chain traceability	Ocean Protocol enabling ML on blockchain-based data marketplaces	Google Nest devices using ML for personalized automation

Singh et al. [39], Alkalbani et al. [40] have applied blockchain to IoT networks to ensure data immutability and traceability. However, many of these solutions suffer from high latency and scalability bottlenecks due to the use of public blockchains and heavy consensus protocols (e.g., Proof-of-Work), making them unsuitable for real-time applications. In addition, most studies assume reliable connectivity and fail to consider the computational limitations of edge devices. For example, [41] propose a blockchain-based energy grid monitoring system but do not account for constrained device resources or bandwidth optimization.

In contrast, our proposed solution introduces a lightweight, permissioned blockchain framework using (e.g., PBFT or Raft consensus) that is specifically tailored to resource-constrained IoT environments. Our approach also integrates off-chain storage and edge computing to enhance scalability and support real-time analytics, limitations not adequately addressed in the above works. In contrast to state-of-the-art systems [42] that use PoW-based public chains, our framework significantly reduces computational overhead while ensuring decentralized trust and immutability. Furthermore, we integrate off-chain data processing and lightweight identity management to support secure, scalable, and fast authentication in heterogeneous IoT environments. The result is a more efficient blockchain solution tailored for IoT security, with the potential to outperform existing models in terms of throughput, responsiveness, and resource efficiency.

Despite significant research in IoT security, there is a lack of integrated frameworks that both secure data integrity and provide intelligent real-time anomaly detection. Existing ML-based detection systems often assume trusted data inputs and overlook vulnerabilities in the data collection process, while blockchain-based approaches rarely extend to deep learning-based classification. This fragmented approach leaves a critical gap in securing end-to-end IoT networks. Our research addresses this problem by proposing a dual-layer privacy-preserving framework: first, using a blockchain-based PoM protocol to ensure tamper-resistant data collection; second, applying a Quantum-inspired Complex CNN, optimized through the HGSOA, to detect and classify malicious activities. This work bridges a documented literature gap by integrating blockchain with optimized ML models to solve the unresolved challenge of secure, intelligent, and scalable IoT anomaly detection.

3 Proposed method

The optimized (PSF-BCH-QICCN-IoT) is discussed. The block diagram of the proposed method (PSF-BCH-QICCN-IoT) is presented in Fig. 1. Figure 1 illustrates a two-level

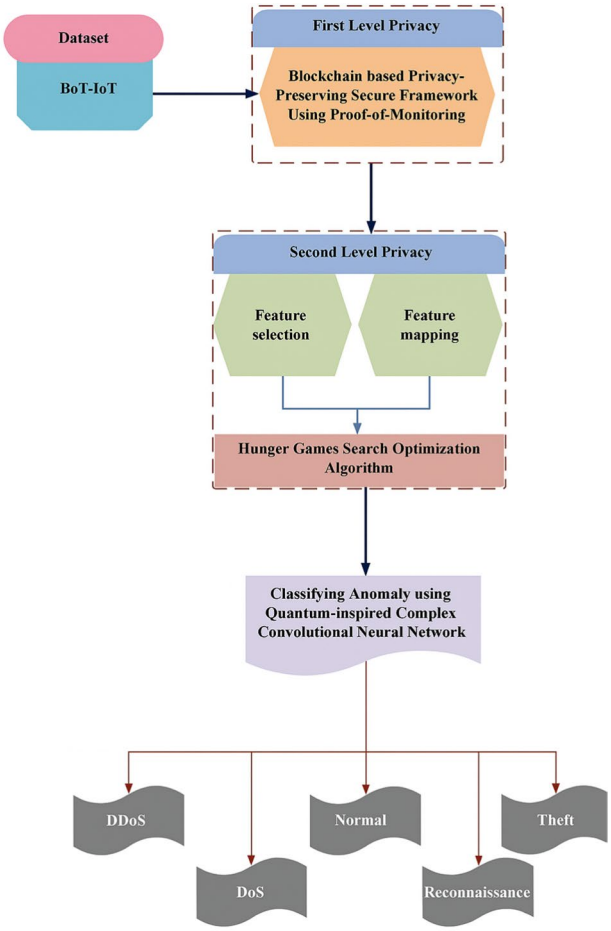


Fig. 1 Block diagram for proposed (PSF-BCH-QICCN-IoT) method

privacy-preserving framework for anomaly detection in IoT networks using the BoT-IoT dataset. At the first level, a blockchain-based privacy-preserving secure framework leveraging a PoM mechanism is used to ensure data integrity and trust. The second level focuses on the privacy-preserving feature engineering through feature selection and feature mapping, which are optimized using HGSOA. The processed features are then fed into a QICCN for anomaly classification. The final output categorizes network behavior into five classes: DDoS, DoS, Normal, Reconnaissance, and Theft, enabling secure and intelligent intrusion detection in IoT environments. Data acquisition; blockchain, feature mapping, feature selection, classification, and optimization are five processes that make up this method. Thus, a full explanation of all steps is provided in the following.

3.1 Data acquisition

In UNSW Canberra's Cyber Range Lab, an accurate network environment was designed to create the BoT-IoT dataset [43]. The botnet and legitimate traffic coexisted

in the network environment. The source files for the data set are accessible in a variety of forms, comprising csv files, formed argus files, and original pcap files. To aid in labeling process, files were separated into subcategories, assault categories. The 69.3 GB gathered pcap files include almost 72.000.000 records. The flow traffic extracted has a size of 16.7 GB in csv format. The data set includes attacks such as DDoS, DoS, OS, Service Scan, Key logging, and data exhilaration. The DDoS and DoS assaults are classified according to the protocol utilized.

3.2 Blockchain-based privacy-preserving secure framework using proof-of-monitoring

PoM eliminates similar data for storage, guarantees security, and is immutable. The time required for complex calculations to reach a consensus is significant. Although the PoM mining task requires computations, a lot of processing power is not needed to tackle the challenge. But PoM, keys are sent at specific frequency, slightly slows down mining process. Consequently, classify PoM's security bound as "medium". By comparison, voting-based consensus algorithms have an unnecessarily high transaction throughput. The PoM can process transactions with less energy consumption. Moreover, in PoM, network monitoring the primary purpose of our Secure Service Level Agreement (SSLA) management framework constitutes a fraction of total energy consumption. SSLA defines the security guarantees that a service provider must uphold, ensuring data integrity and confidentiality. SSLA ensures that IoT devices communicate securely by defining clear security requirements and guarantees between the communicating parties. To clarify, the main purpose of the suggested application is network monitoring, the only way to get PoM consensus. The billing is primarily handled by this organization at the end of the monitoring term. Blockchain nodes are rewarded for allocating their resources throughout the monitoring time with a blockchain fee. It also computes the user's losses in the event of a service outage as shown in Eq. 1.

$$H_{COM}(i) = (H_{Service} - H_{BC}) \times \frac{K_{Violation(i)}}{K_{Monitoring}} \times r(i) \tag{1}$$

Here, $K_{Violation(i)}$ denotes the total amount of time that a violation of i^{th} occurred during the monitoring period $K_{Monitoring}$. $H_{Service}$ represents the transaction service, the blockchain is effective in storing hashes defined by H_{BC}. The total compensation charge for each monitoring period is calculated by our system as shown in Eq. 2.

$$H_{Compensation} = \sum_{i=1}^{m} H_{Compensation(i)} \tag{2}$$

Here, the compensation is denoted by $H_{Compensation}$ and is subsequently moved to the customer's wallet at the PPSF termination phase. Subsequently, the product of vectors and consensus vector is checked every time a novel block index is created in the network. The novel valid block index is attached to the transaction if it is verified by more than 13 fog peers in the Eq. 3.

$$H_{CP} = (H_{Service} - H_{BC}) - H_{Compensation} \tag{3}$$

The main purpose is to calculate the rating scores for each monitoring period, the agreement termination session for blockchain nodes, and SPs, respectively. If the system verifies a violation, the reputation scores of the nonviolation reporter decrease, the reputation scores of the violator reporter increase. The reputation score blockchain node rises above a predetermined level, and it is removed from the network. Additionally, at the point in the customer process where they are choosing an SP, updated rating scores of each SP appear in the Web application. As a result, it makes it easier for the client to select the best SP. As a result, the sensor-gathered observational data are kept in IPFS storage layer's DHT together by matching addressable hash. That type of storage guarantees security, is unchangeable, and eliminates redundant data for storage by eliminating similar data.

3.3 Feature mapping and feature selection utilizing hunger games search optimization algorithm

The proposed HGSOA [44] is used for feature selection and feature mapping to convert categorical values into numerical values, and 10 features are selected. The Hunger Games search (HGS) is a metaheuristic algorithm. Its design is influenced by the gathering tendencies and hunger-driven actions of animals. Although the mathematical model of HGS was developed with a basic framework, the performance is extremely competitive. There are two phases to the food and hunger role strategy.

3.3.1 Stepwise process of HGSOA

The step-by-step approach to HGSOA is shown below. To begin with, HGSOA creates a uniformly distributed population. The entire step method is presented below:

Step 1: Initialization The initialization step, cooperative communication individuals, and foraging behavior are characterized as follows and are given in Eq. 4.

$$H = \begin{cases} G_1 = \overrightarrow{H(u)}.(1 + rand()), \sigma_1 < m \\ G_2 = \overrightarrow{X_1}.\overrightarrow{H_c} + \overrightarrow{S}.\overrightarrow{X_2}.|\overrightarrow{H_c} - \overrightarrow{H(u)}|, \sigma_1 > m, \sigma_2 > R \end{cases} \tag{4}$$

Where σ_1 and σ_2 represent random numbers; *rand*() indicates random numbers of normal distribution; *u* represents the current iteration; X_1 and X_2 represents the weights of hunger behavior; H_c represents the best position of best individuals; *m* indicates the constant; *R* represents the variation control.

Step 2: Random generation After initialization, the input weight parameter developed the randomness method. The characteristics of hunger-driven activity are given in Eq. 5.

$$\bar{f} = 2 \times \alpha\beta - \alpha \tag{5}$$

Where $\bar{f}$ indicates the range of numbers; β represents the random number interval [0,1] ; α represents shrink of iterations.

Step 3: Fitness function We have explicitly defined the fitness function used in our implementation. For our problem domain, the fitness function is formulated as follows.

$$f(x) = 1 - Accuracy(x) \tag{6}$$

where *x* represents the solution vector (e.g., selected feature set or hyperparameter configuration), and accuracy is evaluated using cross-validation in the training set. The goal is to minimize *f*(*x*), thus maximizing accuracy. It is generated from initialized assessments. The fitness function is evaluated using the values of the optimum parameters randomly selected to optimize the weight parameter and it is stated in Eq. 7.

$$fitness\ function = [features\ selection + feature\ mapping] \tag{7}$$

Step 4: Exploration phase for optimizing The features of activities motivated by hunger are reproduced. Consequently, the weights associated with hunger behavior are shown in Eq. 8.

$$\overrightarrow{X_1(m)} = \begin{cases} \delta(j).\sum^{A_{pop/\delta}} \times \sigma_4, \sigma_3 < f^{(l)} \\ 1,\ \sigma_3 > m \end{cases} \tag{8}$$

Where δ represents the hunger of each population; A_{pop} indicates the number of populations; σ denotes random numbers.

Step 5: Exploitation phase for optimizing Exploitation is the final step; the HGSOA selects the uncorrelated features. The control of the variation of each population is given in Eq. 9.

$$\delta(new) = \begin{cases} \delta(G) \times (1 + g_j^{(l)}), \delta_{temp} < \delta(G) \\ \delta_{temp}, \delta_{temp} \geq \delta(G) \end{cases} \tag{9}$$

Where $\delta(new)$ represents the new hunger; $\delta(G)$ represents the largest space bounds; δ represents the hunger of each population.

Step 6: Termination In this step, HGSOA completes the best solution obtained through each iteration of the process returned as output. Finally, HGSOA selects 10 features such as F6, F11, F1, F5, F10, F2, F8, F4, F7 and F9 feature mapping converts categorical values to numerical values. The selected features are given to classification.

3.4 Quantum-inspired complex convolutional neural network

In this section, the QICCN [45] method is proposed for the classification of anomalies. QICCN are kind of DNN that is frequently used for image classification. They are made up of several layers, including convolutional layers for extracting image features with fully connected layers for classification. QICCN is used to classify anomalies such as DDoS, DoS, Normal, Reconnaissance, and Theft. Following the optimization of the dataset, a QICCN based Light GBM approach is implemented as a utility system on the resulting main component. First, Light GBM integrates numerous "weak" learners into a single "strong" learner and makes it easy to acquire "weak" learners, which is the rationale behind its use in the proposed PPSF architecture. Second, numerous learners are more capable of generalizing than a single learner. The use of QICCN for data classification has the potential to develop classification and differentiation in data-related patterns related to the smart city, thus helping to detect processes. Depending on the design in the preceding subsection, resized and better image samples are divided into a training set and a validation set. QICCN method was utilized to input samples for training and validation. The trained method was used to test the set of images for forecast; classification outcome was output for performance evaluation. The detection of normal data was calculated in Eq. 10.

$$||\phi|| = t^{i\lambda}(normal||G_1|| + t^{i\phi} attack||G_2||) \tag{10}$$

Where $||\phi||$ the sigmoid detection of the data calculation, $t^{i\lambda}$ is the threshold value in the data, $normal||G_1||$ is the first detection of the data, $t^{i\phi}$ is the sigmoid threshold value, $attack||G_2||$ is the second detection of the data. Then the accurate value of the enhanced data is calculated in Eq. 11.

$$F(\wp) = t^{y\wp} = normal + attack \tag{11}$$

Where $F(\wp)$ is the accurate value of enhanced data, $t^{y\wp}$ is the accurate threshold value in the image, $normal + attack$ is the calculation of the data. Then the accurate detection of the variation is calculated in Eq. 12.

$$H.G(\wp_2) = \nu(normal + attack)G \tag{12}$$

Where $H.G(\wp_2)$ is accurate variation detection, ν variation, G is data detection, $\nu(normal + attack)G$ is data classification variation detection. The changes in data accuracy are then calculated in Eq. 13.

$$e(\frac{\lambda}{2}F - \wp) = \int_{attack+normal}^{normal-attack} \tag{13}$$

Where e are the changes, $\frac{\lambda}{2}F - \wp$ is the calculation of the accurate value of the enhanced data, $\int_{attack+normal}^{normal-attack}$ is the calculation of the detection of classified data. Then the improved detection is calculated in Eq. 14.

$$\sum = \sum_{s=1}^{S} e(\nu_s)e(\frac{\gamma}{2}y_d) - e(z) \tag{14}$$

Where $\sum$ are the search attacks, $\sum_{s=1}^{S}$ is the storage ensures security, y_d is the detection in acquired data, $e(z)$ is the classification of anomaly data. Although QICCN has previously shown promise in domains such as medical image analysis (e.g., COVID-19 detection), their ability to model complex data relationships and high-dimensional features makes them suitable for IoT anomaly detection as well. In our proposed method, QICCN is adapted and optimized using the Hunger Games Search Algorithm to classify various types of network traffic anomalies - namely, DoS, DDoS, Normal, Reconnaissance, and Theft—based on features derived from the BoT-IoT dataset.

3.5 Optimized using firebug swarm optimization algorithm

The QICCN weight parameter $\wp$ and t is optimized using FSO [46] for an accurate classification. The two basic behavioral patterns of firebugs (Pyrrhocoris apterus) are solitary exploration and roaming, or gregarious behavior in the form of aggregations. These gatherings aid in the firebugs' ability to fend off predators and locate appropriate partners for procreation. Firebugs gather in these groups during the summer. It makes sense to see firebug movement as an optimization process as they search for the ideal partner. Firebugs exhibit wide complex behaviors; therefore it is significant to classify ones that are pertinent to searches.

3.5.1 Stepwise procedure of FSO

The stepwise process is defined to get the ideal value of QICCN depending on the FSO. Initially, FSO makes an equally distributed populace to improve the optimum parameter $\wp$ and t of QICCN. The ideal solution is promoted using the FSO algorithm, the flow diagram is given in Fig. 2.

Step 1: Initialization Every female bug's initialize location is regarding uniform vector random variable within search space. Fit bugs need to be connected to low cost values since firebugs look for mates who share their interests, the objective is to minimize cost function. Using effective Hadamard multiplication processes to find bugs in a certain colony (15).

$$\begin{cases} H_a \leftarrow R_epmat(\nu(\nu), y, 1, T_k) \\ H_b \leftarrow R_epmat(\nu(c), y, 1, T_k) \end{cases} \tag{15}$$

Where H_a is a random number in the range of 1 and c. The function $R_epmat(\nu(c), y)$ returns a matrix with m copies of A along the dimension of the column of the row. Thus, $R_epmat(\nu(\nu), y, 1, T_k)$ yields a matrix.

Step 2: Random generation The input parameters are produced. The individual bugs' fitness was ignored. The update equation is given by:

$$X_i(t+1) = X_i(t) + \alpha.r_1.(G_{best} - X_i(t) + \beta.r_2.(X_j(t) - X_k(t)) \tag{16}$$

Where $X_i(t)$ is the position of the i^{th} firebug in iteration t, G_{best} is the global best position, $X_j(t)$ and $X_k(t)$ are randomly selected firebugs for social interaction, α and β are control parameters, $r_1, r_2 \in [0, 1]$ are random numbers to introduce stochasticity.

Step 3: Estimation of the fitness function Initialized assessments are used to create a random solution. The optimization value of the parameter is evaluated to improve the weight parameter $\wp$ and t of the classifier. It is calculated by Eq. 17,

$$fitness\ function = optimizing[\wp\ and\ t] \tag{17}$$

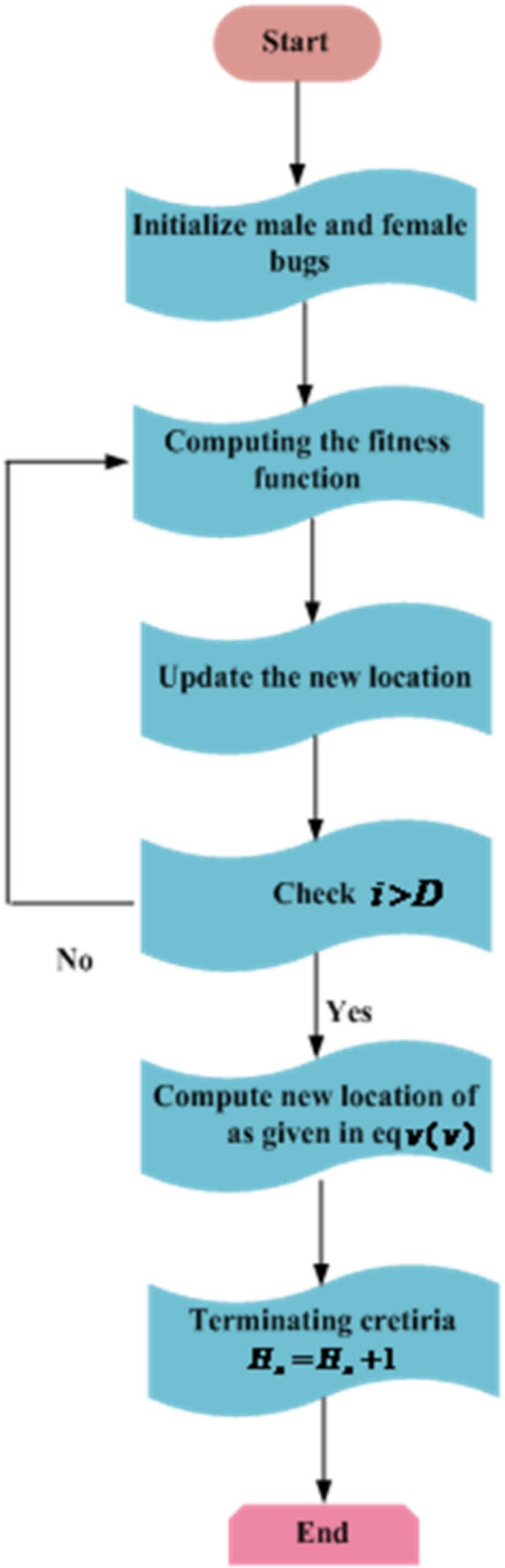


Fig. 2 Flowchart of FSO for enhancing QICCN parameter

The FSO algorithm optimizes the QICCN parameters by minimizing a fitness function defined as:

$$f(X_i) = 1 - Accuracy(X_i) \tag{18}$$

Step 4: Updating swarm activity The following mathematical derivation yields the most basic updating equations for the swarming activity of firebugs.

$$z = (1-\alpha)z^1 + (z^2 - z^1) \tag{19}$$

It is evident from the explanation above that a male bug $(z^2 - z^1)$ is migrating in the direction of the fit female. The authors proposed replacing the scalar α with the column matrix, scalar-vector multiplication with element-wise Hadamard multiplication to improve both independent and scalar exploration in multiple dimensions.

Step 5: Exploration The aforementioned update causes each female bug to migrate weakly towards random male bugs and strongly towards the dominant male bug in charge of the colony since the values in D_1 are selected to be much larger than D_2. The update movement is indicated by the following Eq. 20.

$$\nu(\nu).K \leftarrow \nu(\nu).T + D_1(H_a - \nu(\nu)).F + D_2(H_a - \nu(\nu)).F \tag{20}$$

When D_2 was maintained to be smaller than D_1, the FSO algorithm was found to operate noticeably better in this case. To facilitate exploration, female bugs are drawn to random males. If *a* is any random number between 1 and *b*, the position is denoted by ν.

Step 6: Exploitation phase to optimize $\wp$ and t Similarly, a female bug's great attraction to its dominant male bug and its mild attraction to any random male bug might be described as in Eq. 21.

$$\nu(\nu).z \leftarrow \nu(\nu).z + D_1(\nu(d), z) \tag{21}$$

Where $\nu(\nu).z$ represents the dimension function, $\nu(d)$ defines the male bug might. Based on observations of firebug reproductive swarming activity, in which individual beetles search for the best mates for reproduction, the FSO algorithm was inspired by biology. It makes sense to think of this search for the ideal reproductive partners as a search for the best answers within a search space.

Step 7: Termination The weight parameter values of generator $\wp$ and t from multimodal contrast domain sharing Generative Adversarial Networks optimized using the FSO process will repeat iteratively step 3

until stopping criteria $H_a = H_1 + 1$. Then, finally, PSF-BCH-QICCN-IoT classifies the anomaly with greater accuracy by reducing the false alarm rate with error.

4 Experimental results with discussion

The experimental results of (PSF-BCH-QICCN-IoT) are discussed. The (PSF-BCH-QICCN-IoT) approach is implemented in Python on a HP pavilion laptop through 1TB HDD, 8 GB RAM, 2.67 GHz CPU in windows 10 environment. Several performance matrix are obtained like accuracy, specificity, recall, precision, F1-score, false alarm rate. The results obtained from the proposed (PSF-BCH-QICCN-IoT) technique are analyzed with existing techniques, such as PSF-BCH-GBAD-IoT, PSF-BCH-PCA-IoT, and PSF-BCH-LSTMAE-IoT, respectively.

4.1 Performance measures

The performance of the proposed method is examined using performance metrics such as accuracy, specificity, recall, precision, F1-score, and false alarm rate.

4.1.1 Accuracy

It is accurate to predict disease rather than their status rate. Accuracy serves as a proxy for the general accuracy of the information gathered. It represents the ratio of true positives and true negatives to all occurrences in the dataset. It is measured through Eq. 22.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{22}$$

Here, true positive denotes the disease that is properly anticipated as normal. False positive, or incorrectly diagnosed as afflicted, is known as FP. TN stands for true negative disease or accurately estimated disease as impacted. False negative, or incorrectly projected illness as normal, is FN.

4.1.2 Precision

The degree of accuracy of the data that was obtained is measured by precision. It is a proportion of "true positives" to all "positive instances," where "true positives" refer to the number of correctly returned results. The precision is computed using Eq. 23,

$$Precision = \frac{TP}{TP + FP} \tag{23}$$

4.1.3 Specificity

The percentage of true negatives that the technique correctly identifies is called specificity. It is shown in Eq. 24,

$$Specificity = \frac{TN}{TN + FP} \tag{24}$$

4.1.4 Recall

Recall finds the proportion of positive instances and it is shown in Eq. 25,

$$Recall = \frac{TN}{TN + FN} \tag{25}$$

4.1.5 F1-score

The harmonic means of sensitivity and precision. It is calculated by Eq. 26

$$F1 - score = 2 * \frac{Precision * Recall}{Precision + Recall} \tag{26}$$

4.2 Performance analysis

Figures 3-8 depict the simulation results of the (PSF-BCH-QICCN-IoT) technique. The proposed PMU-SSGCN-HIRS method is likened to existing PSF-BCH-GBAD-IoT, PSF-BCH-PCA-IoT, and PSF-BCH-LSTMAE-IoT methods.

Figure 3 shows the accuracy analysis. Here, (PSF-BCH-QICCN-IoT) method attains $25.21\%, 31.22\%$ and 26.21% high accuracy for DDoS; $23.10\%, 32.53\%$ and 36.40% high accuracy for DoS; $33.24\%, 35.21\%$ and 26.44% high accuracy for Normal; $37.24\%, 31.23\%$ and 36.24% high accuracy for Reconnaissance; $26.36\%, 33.44\%$ and 21.28% high

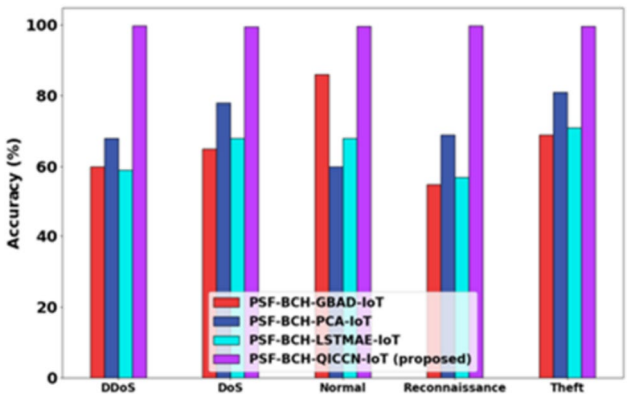


Fig. 3 Accuracy analysis

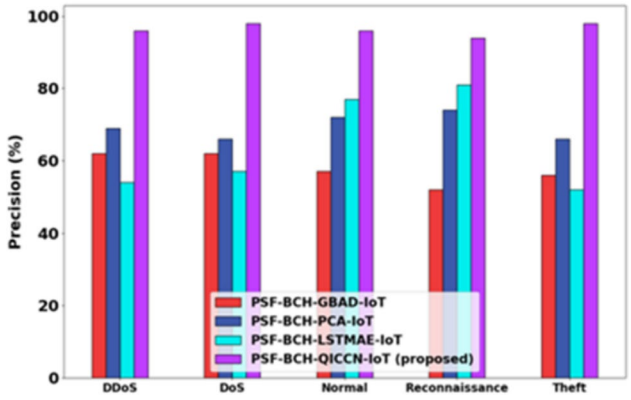


Fig. 4 Precision analysis

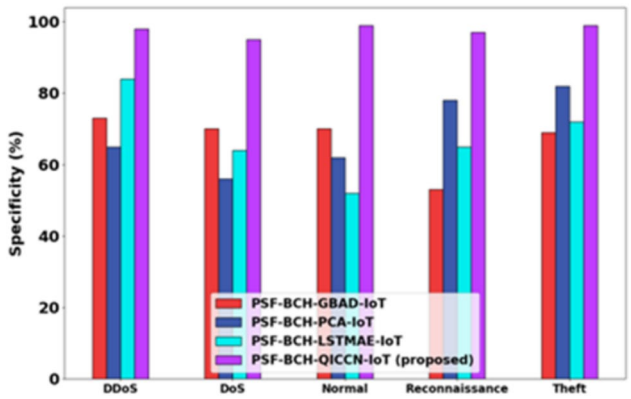


Fig. 5 Specificity analysis

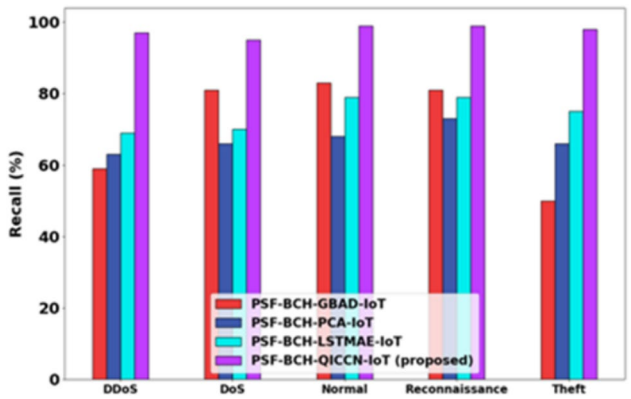


Fig. 6 Recall analysis

accuracy for theft estimated to the existing method such as PSF-BCH-GBAD-IoT, PSF-BCH-PCA-IoT, PSF-BCH-LSTMAE-IoT methods.

Figure 4 shows the precision analysis. Here, (PSF-BCH-QICCN-IoT) method attains $32.21\%, 34.23\%$ and 37.20% high precision for DDoS; $19.40\%, 21.42\%$ and 23.45% high precision for DoS; $24.34\%, 36.28\%$ and 34.43% high precision for Normal; $35.24\%, 33.26\%$ and 27.24% high precision for Reconnaissance; $26.33\%, 35.42\%$ and 28.22% high precision for theft estimated to the existing method such as PSF-BCH-GBAD-IoT, PSF-BCH-PCA-IoT, PSF-BCH-LSTMAE-IoT methods.

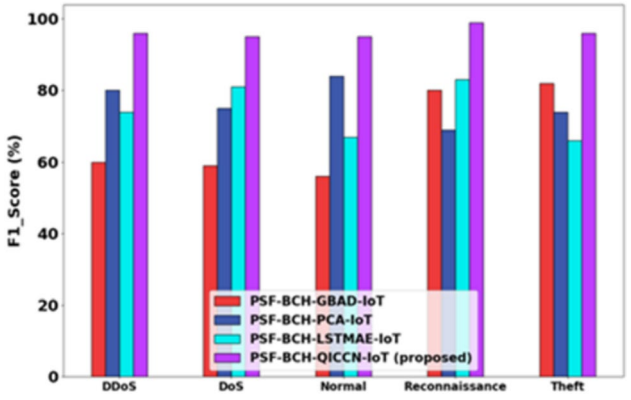


Fig. 7 F1-score analysis

Figure 5 shows a specificity analysis. Here, (PSF-BCH-QICCN-IoT) method attains $35.22\%, 31.21\%$ and 27.20% high specificity, for DDoS; $29.20\%, 35.43\%$ and 26.30% high specificity for DoS; $23.35\%, 30.23\%$ and 31.41% high specificity for Normal; $35.23\%, 31.22\%$ and 24.23% high specificity for Reconnaissance; $25.37\%, 39.45\%$ and 24.29% high specificity for Theft estimated to the existing method such as PSF-BCH-GBAD-IoT, PSF-BCH-PCA-IoT, PSF-BCH-LSTMAE-IoT methods.

Figure 6 shows this recall analysis. Here, (PSF-BCH-QICCN-IoT) method attains $38.29\%, 32.24\%$ and 23.30% high recall, for DDoS; $21.32\%, 33.41\%$ and 26.44% high recall for DoS; $23.34\%, 36.23\%$ and 36.42% high recall for Normal; $36.22\%, 31.24\%$ and 25.21% high recall for Reconnaissance; $26.30\%, 35.19\%$ and 28.28% high recall for Theft estimated to the existing method such as PSF-BCH-GBAD-IoT, PSF-BCH-PCA-IoT, PSF-BCH-LSTMAE-IoT methods.

Figure 7 shows the analysis of the F1-score. Here, (PSF-BCH-QICCN-IoT) method attains $20.23\%, 34.21\%$ and 37.20% high F1-score, for DDoS; $33.40\%, 32.43\%$ and 29.44% high F1-score for DoS; $29.32\%, 34.20\%$ and 39.24% high F1-score for Normal; $37.20\%, 33.23\%$ and 29.22% high F1-score for Reconnaissance; $22.32\%, 31.24\%$ and 29.38% high F1-score for theft estimated to the existing method such as PSF-BCH-GBAD-IoT, PSF-BCH-PCA-IoT, PSF-BCH-LSTMAE-IoT methods.

Figure 8 shows a false alarm rate analysis. Here, (PSF-BCH-QICCN-IoT) method attains $23.12\%, 22.21\%$ and 17.20% low false alarm rate, for DDoS; $13.10\%, 22.43\%$ and 26.14% low false alarm rate for DoS; $23.04\%, 32.22\%$ and 36.44% low false alarm rate for Normal; $26.24\%, 23.20\%$ and 21.29% low false alarm rate for Reconnaissance; $26.30\%, 35.43\%$ and 28.28% low false alarm rate for Theft estimated to the existing method such as PSF-BCH-GBAD-IoT, PSF-BCH-PCA-IoT, PSF-BCH-LSTMAE-IoT methods.

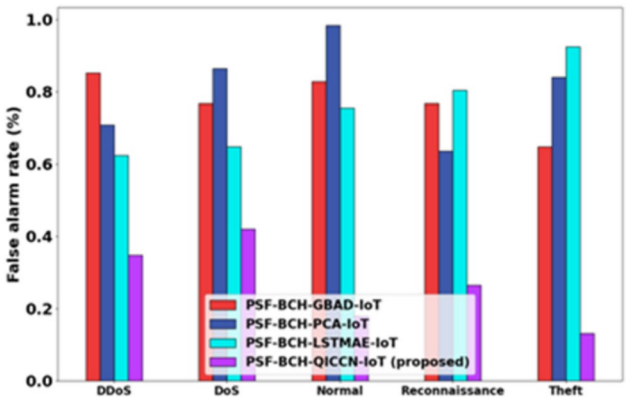


Fig. 8 False alarm rate analysis

4.3 Discussion

In this work, (PSF-BCH-QICCN-IoT) is proposed. A PoM method that depends on the blockchain with smart contracts for data integrity verification and an HGSOA-dependent transformation method to convert data into a novel format were created with privacy preservation in mind. Due to its resistance to inference and data poisoning assaults, the two-level privacy preservation strategy outperforms current efforts in terms of efficiency. Then, using transformed (after utilizing the privacy-preservation method) BoT-IoT based IoT network datasets, a QICCN based Light-GBM was created and assessed. In order to implement the suggested framework, additionally create IoT-fog-cloud incorporated architecture by blockchain-PoM. The results showed that compared to peer privacy-preserving intrusion detection methods, the proposed (PSF-BCH-QICCN-IoT) framework performs better. In the future, this effort will be expanded to include the creation of a prototype to gauge the effectiveness of the suggested framework.

We compare our proposed blockchain-based QICCN framework with three recent and relevant models: SF-BCH-GBAD-IoT, PSF-BCH-PCA-IoT, and PSF-BCH-LSTMAE-IoT. These models represent state-of-the-art approaches that integrate blockchain with various anomaly detection mechanisms in IoT environments. SF-BCH-GBAD-IoT utilizes statistical methods, while PSF-BCH-PCA-IoT and PSF-BCH-LSTMAE-IoT incorporate dimensionality reduction and deep learning, respectively. All models were evaluated in the BoT-IoT dataset using consistent metrics (Accuracy, Precision, Recall, and F1-score). Our method shows superior performance due to its use of a Quantum-inspired Complex CNN optimized by the Hunger Games Search Algorithm, enabling better feature representation and more accurate anomaly classification. This comparison validates our method as a competitive and advanced solution for blockchain-enhanced IoT security.

In order to protect the privacy of user data, we incorporated a blockchain-based algorithm to verify data storage that provides a way to improve data security, consistency, and integrity in a smart city environment. Sensitive information is kept private during model training thanks to this technique. To be more precise, data leakage is avoided by updating the model parameters locally and sharing only aggregated gradients with the server. In order to facilitate distributed learning among edge devices without centralized data collection, the CNN model was altered. The blockchain-based algorithms are integrated with the CNN model to ensure that no raw data is shared during training and that individual data points remain confidential.

5 Conclusion

In this paper, (PSF-BCH-QICCN-IoT) is successfully implemented. The proposed approach (PSF-BCH-QICCN-IoT) is implemented in Python usage of the UNSW-NB15 dataset. The performance of the proposed approach (PSF-BCH-QICCN-IoT) achieves $20.16\%, 31.22\%$ and 28.15% higher specificity; $17.22\%, 23.07\%$ and 19.27% low false rate; $31.33\%, 28.31\%$ and 41.32% higher F1-score compared to existing methods such as PSF-BCH-GBAD-IoT, PSF-BCH-PCA-IoT, PSF-BCH-LSTMAE-IoT, respectively.

Author Contributions Chandra Prakash Singh contributed to Methodology, validation, data curation, writing-original draft. Rohita Yamaganti contributed to project administration. Lokendra Singh Umrao contributed to conceptualization, formal analysis, supervision, write-reviewing, and editing. All authors read and approved the final manuscript.

Funding This research did not receive external funding.

Data Availability No datasets were generated or analysed during the current study.

Materials availability Not applicable.

Code availability Not applicable.

Declarations

Conflict of interest The authors have declared that they have no conflict of interest in this work.

Ethics approval and consent to participate The work submitted is original, and the manuscript has not been submitted to another journal for simultaneous consideration.

Consent for publication The authors declare that they consent to publish the article.

Competing interests The authors declare no competing interests.

References

1. Nations U (2018) World urbanization prospects: The 2018 revision, un department of economic and social affairs. Online. https://population.un.org/wup/
2. Rahman A, Islam MJ, Montieri A, Nasir MK, Reza MM, Band SS, Pescape A, Hasan M, Sookhak M, Mosavi A (2021) Smartblock-sdn: an optimized blockchain-sdn framework for resource management in iot. IEEE Access 9:28361–28376. https://doi.org/10.1109/ACCESS.2021.3058244
3. Huang C, Xue L, Liu D, Shen X, Zhuang W, Sun R, Ying B (2022) Blockchain-assisted transparent cross-domain authorization and authentication for smart city. IEEE Internet Things J 9(18):17194–17209. https://doi.org/10.1109/JIOT.2022.3154632
4. Malik H, Anees T, Faheem M, Chaudhry MU, Ali A, Asghar MN (2023) Blockchain and internet of things in smart cities and drug supply management: open issues, opportunities, and future directions. Internet of Things 23:100860. https://doi.org/10.1016/j.iot.2023.100860
5. Latif S, Idrees Z, Ahmad J, Zheng L, Zou Z (2021) A blockchain-based architecture for secure and trustworthy operations in the industrial internet of things. J Ind Inf Integr 21:100190. https://doi.org/10.1016/j.jii.2020.100190
6. Tripathi AM, Umrao LS (2025) Integrated fuzzy decision tree based blockchain federated safety-as-a-service for iiot. Clust Comput 28(95):1–12. https://doi.org/10.1007/s10586-024-04835-3
7. Kayode Saheed Y, Harazeem Abdulganiyu O, Ait Tchakoucht T (2023) A novel hybrid ensemble learning for anomaly detection in industrial sensor networks and scada systems for smart city infrastructures. J King Saud Univ Comput Inf Sci 35(5):101532. https://doi.org/10.1016/j.jksuci.2023.03.010
8. Kayode Saheed Y, Ebere Chukwuere J (2025) Cps-iiot-p2attention: Explainable privacy-preserving with scaled dot-product attention in cyber-physical system-industrial iot network. IEEE Access 13:81118–81142. https://doi.org/10.1109/ACCESS.2025.3566980
9. Egala BS, Pradhan AK, Badarla V, Mohanty SP (2021) Fortified-chain: a blockchain-based framework for security and privacy-assured internet of medical things with effective access control. IEEE Internet Things J 8(14):11717–11731. https://doi.org/10.1109/JIOT.2021.3058946
10. Tao X, Das M, Liu Y, Cheng JCP (2021) Distributed common data environment using blockchain and interplanetary file system for secure bim-based collaborative design. Autom Constr 130:103851. https://doi.org/10.1016/j.autcon.2021.103851
11. Han P, Zhang Z, Ji S, Wang X, Liu L, Ren Y (2023) Access control mechanism for the internet of things based on blockchain and inner product encryption. Journal of Information Security and Applications 74:103446. https://doi.org/10.1016/j.jisa.2023.103446
12. Abdulganiyu OH, Ait Tchakoucht T, Alaoui AEH, Saheed YK (2025) Attention-driven multi-model architecture for unbalanced network traffic intrusion detection via extreme gradient boosting. Intell Syst Appl 26:200519. https://doi.org/10.1016/j.iswa.2025.200519
13. Adeyiola AQ, Saheed YK, Misra S, Chockalingam S (2023) Metaheuristic firefly and c5.0 algorithms based intrusion detection for critical infrastructures. In: 2023 3rd International Conference on Applied Artificial Intelligence (ICAPAI), pp 1–7. https://doi.org/10.1109/ICAPAI58366.2023.10193917
14. Qahtan S, Sharif KY, Zaidan AA, Alsattar HA, Albahri OS, Zaidan BB, Zulzalil H, Osman MH, Alamoodi AH, Mohammed RT (2022) Novel multi security and privacy benchmarking framework for blockchain-based iot healthcare industry 4.0 systems. IEEE Trans Ind Inform 18(9):6415–6423. https://doi.org/10.1109/TII.2022.3143619
15. Jabbar R, Fetais N, Kharbeche M, Krichen M, Barkaoui K, Shinoy M (2021) Blockchain for the internet of vehicles: How to use blockchain to secure vehicle-to-everything (v2x) communication and payment? IEEE Sens J 21(14):15807–15823. https://doi.org/10.1109/JSEN.2021.3062219
16. Josphine CV, Kingslin MT, Vincy RF, Mohana M, Babitha S (2024) Efficient quantum inspired blockchain-based cyber security framework in iot using deep learning and huristic algorithms. Intell Decis Technol 18(2):1203–1232. https://doi.org/10.3233/IDT-230579. https://journals.sagepub.com/doi/pdf/10.3233/IDT-230579
17. Saheed YK, Misra S (2025) Cps-iot-ppdnn: A new explainable privacy preserving dnn for resilient anomaly detection in cyber-physical systems-enabled iot networks. Chaos, Solitons & Fractals 191:115939. https://doi.org/10.1016/j.chaos.2024.115939
18. Yaseen H, Hassan SI (2024) A systematic review on privacy preservation techniques for smart contracts in blockchain using machine learning. In: 2024 International Conference on Cognitive Robotics and Intelligent Systems (ICC - ROBINS), pp 822–827. https://doi.org/10.1109/ICC-ROBINS60238.2024.10533967
19. Singh CP, Yamaganti R, Umrao LS (2025) Variational onsager neural networks-based fair proof-of-reputation consensus for blockchain with transaction prioritisation for smart cities. J Supercomput 81(97):1–23. https://doi.org/10.1007/s11227-024-06626-4
20. Singh P, Masud M, Hossain MS, Kaur A (2021) Blockchain and homomorphic encryption-based privacy-preserving data aggregation model in smart grid. Comput Electr Eng 93:107209. https://doi.org/10.1016/j.compeleceng.2021.107209
21. Kumar R, Javeed D, Aljuhani A, Jolfaei A, Kumar P, Islam AKMN (2024) Blockchain-based authentication and explainable ai for securing consumer iot applications. IEEE Trans Consum Electron 70(1):1145–1154. https://doi.org/10.1109/TCE.2023.3320157
22. Sharma C, Batra I, Sharma S, Malik A, Hosen ASMS, Ra I-H (2022) Predicting trends and research patterns of smart cities: a semi-automatic review using latent dirichlet allocation (lda). IEEE Access 10:121080–121095. https://doi.org/10.1109/ACCESS.2022.3214310
23. Thapliyal S, Wazid M, Singh DP, Das AK, Shetty S, Alqahtani A (2023) Design of robust blockchain-envisioned authenticated key management mechanism for smart healthcare applications. IEEE Access 11:93032–93047. https://doi.org/10.1109/ACCESS.2023.3310264
24. Aliahmadi A, Nozari H (2023) Evaluation of security metrics in aiot and blockchain-based supply chain by neutrosophic decision-making method. Supply Chain Forum An International Journal 24(1):31–42. https://doi.org/10.1080/16258312.2022.2101898
25. Challa R, Kothamasu KK (2024) A decentralized public-permissioned blockchain framework for enhanced security of health records in fog computing. Comput Methods Biomech Biomed Engin 27(13):1832–1844. https://doi.org/10.1080/10255842.2023.2262664. PMID: 37807911
26. Jayabalan J, Jeyanthi N (2022) Scalable blockchain model using off-chain ipfs storage for healthcare data security and privacy. J Parallel Distrib Comput 164:152–167. https://doi.org/10.1016/j.jpdc.2022.03.009
27. Kumar P, Kumar R, Srivastava G, Gupta GP, Tripathi R, Gadekallu TR, Xiong NN (2021) Ppsf: A privacy-preserving and secure framework using blockchain-based machine-learning for iot-driven smart cities. IEEE Trans Netw Sci Eng 8(3):2326–2341. https://doi.org/10.1109/TNSE.2021.3089435
28. Kumar P, Gupta GP, Tripathi R (2021) Tp2sf: A trustworthy privacy-preserving secured framework for sustainable smart cities by leveraging blockchain and machine learning. J Syst Archit 115:101954. https://doi.org/10.1016/j.sysarc.2020.101954

29. Kumar R, Kumar P, Tripathi R, Gupta GP, Kumar N, Hassan MM (2022) A privacy-preserving-based secure framework using blockchain-enabled deep-learning in cooperative intelligent transport system. IEEE Trans Intell Transp Syst 23(9):16492–16503. https://doi.org/10.1109/TITS.2021.3098636
30. Kumar P, Kumar R, Gupta GP, Tripathi R, Srivastava G (2022) P2tif: A blockchain and deep learning framework for privacy-preserved threat intelligence in industrial iot. IEEE Trans Industr Inf 18(9):6358–6367. https://doi.org/10.1109/TII.2022.3142030
31. Ahamad D, Hameed SA (2023) Two level blockchain-based privacy preservation framework in iot with heuristic fusion mechanism-aided deep learning architecture. Internet of Things 24:100917. https://doi.org/10.1016/j.iot.2023.100917
32. Hamouda D, Ferrag MA, Benhamida N, Seridi H (2023) Ppss: A privacy-preserving secure framework using blockchain-enabled federated deep learning for industrial iots. Pervasive Mob Comput 88:101738. https://doi.org/10.1016/j.pmcj.2022.101738
33. Sanghami SV, Lee JJ, Hu Q (2023) Machine-learning-enhanced blockchain consensus with transaction prioritization for smart cities. IEEE Internet Things J 10(8):6661–6672. https://doi.org/10.1109/JIOT.2022.3175208
34. Ali AA, Gunavathie MA, Srinivasan V, Aruna M, Chennappan R, Matheena M (2025) Securing electronic health records using blockchain-enabled federated learning for iot-based smart healthcare. Clinical eHealth 8:125–133. https://doi.org/10.1016/j.ceh.2025.04.002
35. Dorri A, Kanhere SS, Jurdak R, Gauravaram P (2017) Blockchain for iot security and privacy: The case study of a smart home. In: 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), pp 618–623. https://doi.org/10.1109/PERCOMW.2017.7917634
36. Mlika F, Karoui W, Romdhane LB (2024) Trustworthy decentralization based on blockchain tools for social network architectures. Soc Netw Anal Min 14(95):1–28. https://doi.org/10.1007/s13278-024-01252-7
37. Gugueoth V, Safavat S, Shetty S, Rawat D (2023) A review of iot security and privacy using decentralized blockchain techniques. Comput Sci Rev 50:100585. https://doi.org/10.1016/j.cosrev.2023.100585
38. Khrais LT (2020) Iot and blockchain in the development of smart cities. Int J Adv Comput Sci Appl 11(2). https://doi.org/10.14569/IJACSA.2020.0110220
39. Singh S, Sharma PK, Yoon B, Shojafar M, Cho GH, Ra I-H (2020) Convergence of blockchain and artificial intelligence in iot network for the sustainable smart city. Sustain Cities Soc 63:102364. https://doi.org/10.1016/j.scs.2020.102364
40. Alkalbani M, Hamdaoui B, Zorba N, Rayes A (2019) A blockchain-based iot networks-on-demand protocol for responsive smart city applications. In: 2019 IEEE Global Communications Conference (GLOBECOM), pp 1–6. https://doi.org/10.1109/GLOBECOM38437.2019.9013790
41. Kolahan A, Maadi SR, Teymouri Z, Schenone C (2021) Blockchain-based solution for energy demand-side management of residential buildings. Sustain Cities Soc 75:103316. https://doi.org/10.1016/j.scs.2021.103316
42. Sharma PK, Park JH (2018) Blockchain based hybrid network architecture for the smart city. Future Gener Comput Syst 86:650–655. https://doi.org/10.1016/j.future.2018.04.060
43. Koroniotis N, Moustafa N, Schiliro F, Gauravaram P, Janicke H (2020) A holistic review of cybersecurity and reliability perspectives in smart airports. IEEE Access 8:209802–209834. https://doi.org/10.1109/ACCESS.2020.3036728
44. Onay FK, Salih BA (2022) Chaotic hunger games search optimization algorithm for global optimization and engineering problems. Math Comput Simul 192:514–536. https://doi.org/10.1016/j.matcom.2021.09.014
45. Shi S, Wang Z, Cui G, Wang S, Shang R, Li W, Wei Z, Gu Y (2022) Quantum-inspired complex convolutional neural networks. Appl Intell 52(15):17912–1792. https://doi.org/10.1007/s10489-022-03525-0
46. Noel MM, Muthiah-Nakarajan V, Amali GB, Trivedi AS (2021) A new biologically inspired global optimization algorithm based on firebug reproductive swarming behaviour. Expert Syst Appl 183:115408. https://doi.org/10.1016/j.eswa.2021.115408

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.

UNITED INSTITUTE OF MANAGEMENT

NAINI, PRAYAGRAJ

(Approved by AICTE & affiliated to Dr APJ Abdul Kalam Technical University, Lucknow, UP India)

International Conference on

Global Innovative Practices in Sustenance of Modern Businesses

25-26 April 2025

Certificate

This is to certify that Prof/Dr/Mr/Ms Chandra Prakash Singh, Assistant Professor of P.K. University, Shivpuri (M.P.) has participated /presented the paper entitled Blockchain in Smart Cities: Review of Literature in the Conference.

Dr Ajay Kumar Yadav
(Co-Convener)

Prof K K Malviya
(Conference Chair)

UIM/IntConf/2025/166

ECE/RTSEM2025/016

ESHAN COLLEGE OF ENGINEERING, FARAH, MATHURA

NAAC ACCREDITED, APPROVED BY AICTE, NEW DELHI AND AFFILIATED TO AKTU, LUCKNOW

2nd National Conference on Recent Trends in Science, Engineering and Management
(RTSEM-2025)

CERTIFICATE OF PARTICIPATION

Chandra Prakash Singh, P.K.University, Shivpuri (M.P)

Presented the paper titled

A Study : Blockchain based Transaction Prioritization

for Smart City

Co-authored by

Dr.Rohita Yamaganti, Dr. Lokendra Singh Umrao

in the National Conference on Recent Trends in Science, Engineering and Management (RTSEM-2025) held during April 11th-12th, 2025 at Eshan College of Engineering, Farah, Mathura, in association with The Institution of Engineers (India).

Er. Vyom Kulshreshtha Organizing Secretary	D.R.Bansal Convener	Er. Rajneesh Kumar Yadav FIE, Chairman IEI Agra Local Centre	Dr. Pankaj Sharma Director