IJARETY

International Journal of Advanced Research in Education and TechnologY (IJARETY)

Volume 12, Issue 3, May-June 2025

Impact Factor: 8.152

www.ijarety.in editor.ijarety@gmail.com

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN:2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May-June 2025 ||

DOI:10.15680/IJARETY.2025.1203042

Secure and Private Smart Cities using Blockchain Technology

Prathaapani Sai Harshitha, Sabavat Rajashekhar, Muppalla Manideep, Kasi Saialaja

UG Students, Department of CSE, Guru Nanak Institutions Technical Campus, Hyderabad, India

Assistant Professor, Department of CSE, Guru Nanak Institutions Technical Campus, Hyderabad, India

ABSTRACT: Building smart services for smart cities has become a major focus in modern technological advancements. Mobile scanners play a crucial role in capturing and processing data from various sources. Smart city applications emphasize the need for secure data sharing across heterogeneous devices. However, certain actions taken during data sharing can pose risks to security, privacy, and data integrity. The reliance on a centralized repository has been a major factor in past security breaches. Therefore, ensuring secure authentication and the protection of sensitive data is crucial for modern applications. Blockchain is a widely adopted technology that ensures data integrity and security. This paper introduces a novel blockchain-based framework, SecPrivPreserve, designed to enhance the security and integrity of data generated by mobile scanners. The proposed framework secures data through multiple phases, including initialization, registration, data protection, authentication, access control, validation, data sharing, and secure downloads. To strengthen security, SecPrivPreserve integrates various mechanisms such as encryption, hashing, and authentication techniques that enhance confidentiality, privacy, and integrity. Unlike traditional approaches that rely on one-time passwords (OTP) for authentication and data sharing, this framework employs QR codes for secure access and data-sharing keys to further enhance security. Since the SecPrivPreserve framework is built on a permissioned blockchain, it inherently benefits from tamper-proof records and non-repudiation. Moreover, for data protection techniques to enhance cryptographic security.

KEYWORDS: Authentication, blockchain, IoT, security, smart city, smart contracts.

I.INTRODUCTION

Recently, all the nations in the world have been gearing up their services, applications, and infrastructure for the betterment of their people's life using smart technologies. In this context, the Internet of Things (IoT) is crucial for connecting physical devices to the internet using different protocols to facilitate data transfer among diverse places. In recent decades, there has been an enormous necessity for IoT-based services in various sectors such as healthcare, manufacturing, financial services, traffic monitoring, weather monitoring, and energy transfer. Due to their compactness and minimal power consumption, the usage of IoT devices is expected to reach more than $1.4 trillion in 2027. Many countries invest a lot of money in initiatives relating to smart cities. For instance, China is engaged in more than 220 initiatives that aim to create a smart city and improve the quality of life for citizens. Associated technologies for smart cities assist urban municipalities in managing their day-to-day operations. According to IBM, the smart city has three main characteristics instrumented (sensors, actuators), interconnected (information sharing among devices), and intelligent (improve quality of citizens' life). Recent observation reveals that the smart city has substantially enhanced the quality of life and amenities of inhabitants in urban areas. According to a United Nations Population Fund report, more than half of the world's population lives in urban areas. The smart city has caught the attention of both academia and business since it has significantly decreased the logistical problems related to acquiring services. Several cities worldwide have begun to build their own smart city strategies to improve their inhabitants' quality of life. IoT and smart environments have become synonymous.

IoT technology is capable of sensing every entity in the real world, so it finds importance in healthcare, transport, traffic system, public safety, smart building, and smart agriculture. Amid many merits, due to the presence of inconsistent protocol standards, resourceconstrained nature, and centralized repository IoT devices are vulnerable to security and privacy breaches. In a smart environment, people may face security and privacy risks due to the vulnerabilities in smart city applications. For instance, malicious attackers may fabricate data to execute their ill intent, which may jeopardize the decision-making system. In addition, these malicious attackers also make all sorts of attempts to prevent the legitimate users' service by executing denial-of-service (DoS) attacks, transmission, disrupting sensing, and control in order to degrade the quality of intelligent city services. Furthermore, as new devices or software are

| ISSN:2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May-June 2025 ||

DOI:10.15680/IJARETY.2025.1203042

connected, the complexity level of the risks of smart city applications grows, particularly while ensuring privacy. Unfortunately, most protection methods (encryption, authentication mechanism) are insufficient to protect smart city applications against the new dynamic threats. Implementing complex procedures wouldn't be possible since the devices have less computational power. Hence, a simple framework that considers simple cryptography techniques would be an appropriate solution for IoT's heterogeneity and dynamic characteristics is appreciable. Data breaches can occur during data storage, transmission, and sharing, posing significant risks to data owners and providers. Regulations are in place to protect the data source and the system from potential harm caused by target data nodes. As a result, during data transactions, it is imperative that both the source and target nodes comply with the policies and regulations of their respective areas.

Smart cities are built around integrating sensors and smart technologies, allowing citizens and organizations to access data through their smart devices to process and utilize data. However, the utilization of data in smart cities raises privacy concerns, including hacking sensitive data through injecting data poisoning attacks. These attacks could result in the alteration of sensitive data, which in turn leads to the disruption of communication within smart entities. IoT networks in smart cities are particularly susceptible to cyber-attacks that threaten the data integrity, confidentiality, and availability of these systems. To mitigate these risks, smart cities must implement robust security mechanisms to protect their assets against cyber-attacks (Distributed Denial of Service (DDoS), DoS, Man-in-the-Middle, ransomware). The frequency and impact of these attacks emphasize the need for adequate privacy and security measures in smart cities. Researchers have developed many data-securing schemes to offer privacy and security for applications meant for smart cities. Earlier centralized cloud-based data-sharing frameworks have failed to address smart applications' data integrity and privacy issues. However, blockchain-based solutions provide greater improvement in solving privacy issues. Initially, data collected from sensors using a detection algorithm takes client data into various communities based on similarity labels. It has a specific type of control on community data with specifying detection algorithm. However, this framework has not addressed data protection.

II.LITERATURE REVIEW

M. Ramaiah, V. Chithanuru, A. Padma, and V. Ravi, industry 4.0 is a technology initiative intended to improve the efficiency of the task for the smart manufacturing industries. Industry 4.0 encompasses the trending technologies like the Internet of Things, Industrial Internet of Things, Artificial Intelligence, and Big Data analytics and comes up with their challenges while customizing it for the task. Trending smart technologies are no exception to being hacked by cyber security attacks. To facilitate automation, the interconnected devices need robust and intelligent security systems to prevent security breaches anticipated from the anonymous entity. Hence, a clear understanding of various security aspects of Industry 4.0 is very essential to prevent security attacks. This chapter attempts to highlight the possible security vulnerabilities anticipated for Industry 4.0 from its constituent key elements and the possible security solution using blockchain technologies.

X. Yang, R. Zhang, C. Yue, Y. Liu, B. C. Ooi, Q. Gao, Y. Zhang, and H. Yang,, VeDB: A software and hardware enabled trusted relational database, blockchain-like ledger databases emerge in recent years as a more efficient alternative to permissioned blockchains. Conventional ledger databases mostly rely on authenticated structures such as the Merkle tree and transparency logs for supporting auditability, and hence they suffer from the performance problem. As opposed to conventional ledger DBMSes, we design VeDB - a high-performance verifiable software (Ve-S) and hardware (Ve-H) enabled DBMS with rigorous auditability for better user options and broad applications. In Ve-S, we devise a novel verifiable Shrubs array (VSA) with two-layer ordinals (serial numbers) which outperforms conventional Merkle tree-based models due to lower CPU and I/O cost. It enables rigorous auditability through its efficient credible timestamp range authentication method, and fine-grained data verification at the client side, which are lacking in state-of-the-art relational ledger databases. In Ve-H, we devise a non-intrusive trusted affiliation by TEE leveraging digest signing, monotonic counters, and trusted timestamps in VeDB, which supports both data notarization and lineage applications. The experimental results show that VeDB-VSA outperforms Merkle tree-based authenticated data structures (ADS) up to 70× and 3.7× for insertion and verification; and VeDB Ve-H data lineage verification is 8.5× faster than Ve-S.

Private blockchain envisioned access control system for securing industrial IoT-based pervasive edge computing, S. Saha, B. Bera, A. K. Das, N. Kumar, S. H. Islam, and Y. Park, the Industrial Internet of Things (IIoT) is able to connect machines, analytics and people with IoT smart devices, gateway nodes and edge devices to create powerful intuitivenesses to drive smarter, faster and effective business agreements. IIoT having interconnected machines along

| ISSN:2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May-June 2025 ||

DOI:10.15680/IJARETY.2025.1203042

with devices can monitor, gather, exchange, and analyze information. Since the communication among the entities in IIoT environment takes place insecurely (for instance, wireless communications and Internet), an intruder can easily tamper with the data. Moreover, physical theft of IoT smart devices provides an intruder to mount impersonation and other attacks. To handle such critical issues, in this work, we design a new private blockchain-envisioned access control scheme for Pervasive Edge Computing (PEC) in IIoT environment, called PBACS-PECIIoT. We consider the private blockchain consisting of the transactions and registration credentials of the entities related to IIoT, because the information is strictly confidential and private. The security of PBACS-PECIIoT is significantly improved due to usage of blockchain as immutability, transparency and decentralization along with protection of various potential attacks. A meticulous comparative analysis exhibits that PBACS-PECIIoT achieves greater security and more functionality features, and requires low costs for communication and computational as compared to other pertinent schemes.

C. Zhang, M. Zhao, L. Zhu, W. Zhang, T. Wu, and J. Ni,FRUIT: A blockchain-based efficient and privacy-preserving quality-aware incentive scheme, incentive plays an important role in knowledge discovery, as it impels users to provide high-quality knowledge. To promise incentive schemes with transparency, blockchain technology has been widely used in incentive schemes. Currently, privacy, reliability, streamlined processing, and quality awareness are major challenges in designing blockchain-based incentive schemes. In this paper, we design a blockchain-based eFficient and pRivacy-preserving qUality-aware IncenTive scheme called FRUIT. With well-designed smart contracts, FRUIT achieves privacy, reliability, streamlined processing, and quality awareness during the whole procedure. Specifically, we design a novel lightweight encryption method by combining matrix decomposition with proxy re-encryption and a privacy-preserving task allocation based on the polynomial fitting function and hash function. Then, we leverage our proposed lightweight encryption and task allocation to build an efficient and privacy-preserving knowledge discovery protocol in order to securely calculate the data quality and truthful knowledge. To promise user reliability in the incentive scheme, we utilize the Dirichlet distribution to realize the automatic reputation prediction based on the data quality by deploying the reputation management on the blockchain. Moreover, we also deploy the payment management on the blockchain, endowing the incentive scheme to reward participants based on the data quality automatically. Through a detailed security analysis, we demonstrate that data privacy and task privacy are well preserved during the whole process. Theoretical analysis and extensive experiments on real-world datasets demonstrate that FRUIT has acceptable efficiency and affordable performance in terms of computation cost, communication overhead, and gas consumption.

P. M. Kumar, B. Rawal, and J. Gao, Blockchain-enabled privacy preserving of IoT data for sustainable smart cities using machine learning, the development of sensor technologies and an explosion of the inexpensive electronic circuit, the Internet of Things (IoT) is emergent as an encouraging innovation to comprehend sustainable smart city. Smart cities can bid various intelligent applications like smart transportation, smart banking, and industry 4.0, among others, to boost citizens' life quality. However, security is one of the critical problems of a smart city. These emerging smart infrastructure and applications based on IoT can benefit users only if vital private and secure features are guaranteed. Hence, in this paper, Blockchain-enabled Privacy-Preserving Access Control System (BPACS) has been suggested for IoT data in a smart city environment. This study utilizes blockchain methods to construct a reliable and secure data-sharing policy between numerous data providers, where IoT information is encoded and then verified on disseminated ledgers. Furthermore, this study design protected construction blocks, like secure comparison and secure polynomial multiplications, by retaining cryptosystems and build a secure Support Vector Machine (SVM) and Principle Component Analysis (PCA) training algorithms. Hard security analysis proves that the suggested model guarantees the privacy of the sensitive information for every data provider and the SVM and PCA model variables for data analysts.

III.METHODOLOGY OF PROPOSED SURVEY

In the current landscape, IoT devices in smart cities rely heavily on centralized repositories for data storage and management. These repositories store vast amounts of sensitive data collected from various devices, which makes them attractive targets for cyberattacks. The existing systems often depend on traditional security mechanisms such as passwords, basic encryption, and hashing to safeguard data. However, these systems face challenges in maintaining data integrity, preventing unauthorized access, and ensuring privacy across heterogeneous devices. Additionally, centralized systems are vulnerable to issues like single points of failure, tampering, and data breaches, which compromise security and hinder trust in IoT applications.The novel framework consists of seven different phases to successfully store and validate the client data to ensure the various security benefits privacy and integrity. The presented phases taxonomy table is shown in Table 1. Each participant identification number was produced using a random number string and hashed using SHA256, in the initialization phase to initiate the request. In the registration

| ISSN:2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May-June 2025 ||

DOI:10.15680/IJARETY.2025.1203042

phase, different kinds of peers implement the enrollment task using passwords generated through the hashed random number (OTP) and current time. The data protection phase uses the AES algorithm (128-bit key length) to encrypt the client data. To increase the degree of confidentiality, interpolation, and Chebyshev polynomials are also deployed in the data protection phase. The MSP uses hashing to authenticate clients' data by using the digital signature. To facilitate data access control, hashed passwords are used to prevent data tampering. To download the data for verification purposes data sharing downloading is done through AES and Chebyshev polynomials.

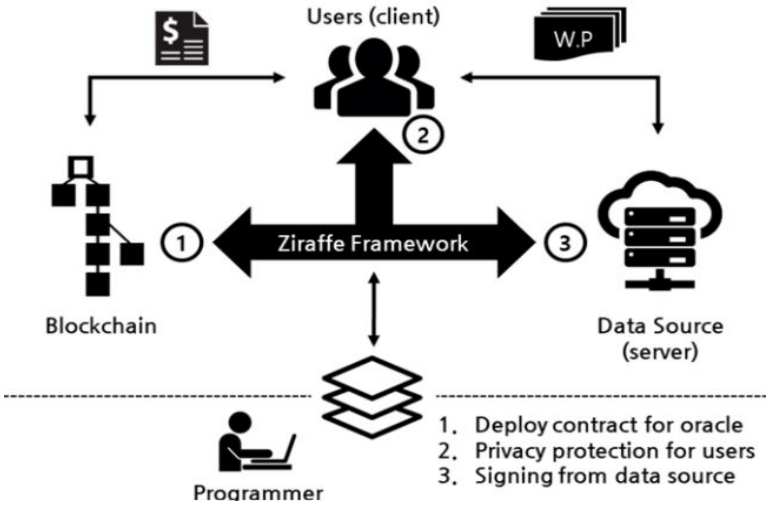

Figure 1. Architecture of the model.

The authors presented a secure Support Vector Machine (SVM) based approach along with blockchain to overcome the security issue of collecting training data from multiple data providers. A homomorphic cryptosystem paillier has been deployed to ensure the confidentiality of the sensitive data collected from various IoT devices and thus created secure building blocks. The system exchanges the learning model in contradiction to data. However, the model still needs to improve the data utility. The authors presented a blockchain-based data sharing and access control system. Here, multiple smart contracts are proposed to secure, authenticate, network management of users, and detect misbehavior of users.

The rapid growth of the Internet of Things (IoT) and the increasing complexity of smart city applications have highlighted significant challenges in ensuring the security, privacy, and integrity of sensitive data shared across heterogeneous devices. Centralized repositories used for data storage have become a major target for cyberattacks, exposing critical information to risks of compromise. In IoT environments, secure data sharing and robust authentication are vital for protecting applications from potential vulnerabilities. Despite the use of various security mechanisms, the integration of IoT and blockchain technologies often faces issues in maintaining data integrity, preventing unauthorized access, and ensuring non-repudiation. Therefore, there is a pressing need for an innovative framework that guarantees the security of IoT data throughout its lifecycle, from collection and authentication to sharing and downloading, while addressing the challenges of centralized data management and ensuring tamper-proof data handling.

The proposed SecPrivPreserve framework introduces a decentralized, blockchain-based approach to enhance the security, privacy, and integrity of IoT data in smart cities. By leveraging the strengths of permissioned blockchain technology, the framework addresses the vulnerabilities of centralized systems by ensuring tamper-proof data storage, non-repudiation, and secure data sharing across IoT devices. It incorporates a variety of security mechanisms, including OTP-based passwords, encryption, hashing, and QR code-based encryption, throughout the data lifecycle—ranging from initialization and registration to data access control, validation, and sharing. This approach not only strengthens the overall security posture of IoT applications but also ensures that sensitive data is protected from unauthorized access and tampering, providing a more reliable and robust solution for smart cities.

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN:2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May-June 2025 ||

DOI:10.15680/IJARETY.2025.1203042

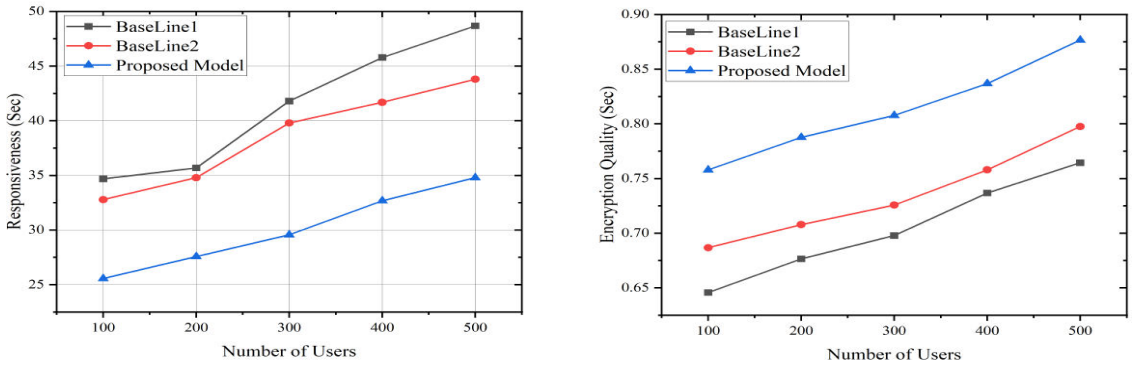

Figure 2. Responsiveness & Encryption quality.

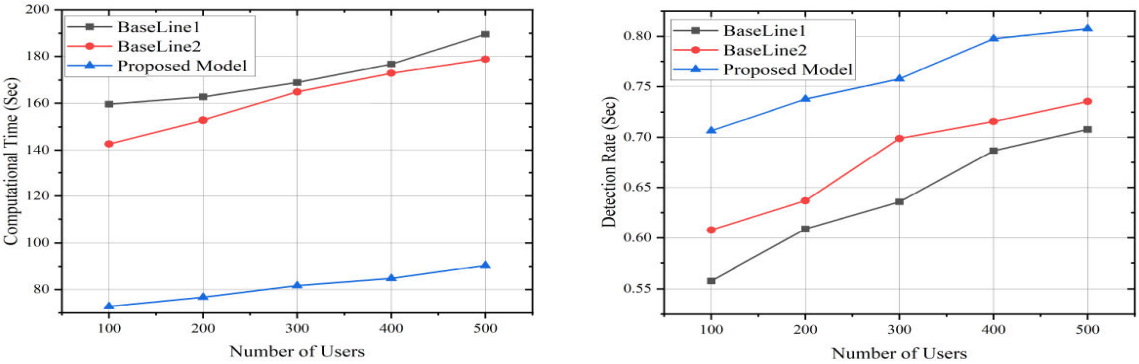

Figure 3. Computational time & Detection rate.

SecPrivPreserve framework

The emergence of the Internet of Things (IoT), Industry 5.0 applications and associated services have caused a powerful transition in the cyber threat landscape. As a result, organisations require new ways to proactively manage the risks associated with their infrastructure. In response, a significant amount of research has focused on developing efficient Cyber Threat Intelligence (CTI) sharing. However, in many cases, CTI contains sensitive information that has the potential to leak valuable information or cause reputational damage to the sharing organisation.

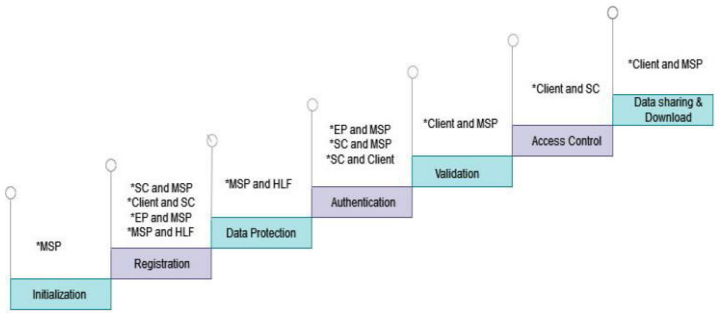

Figure 4. The proposed SecPrivPreserve framework phases.

While a number of existing CTI sharing approaches have utilised blockchain to facilitate privacy, it can be highlighted that a comprehensive approach that enables dynamic trust-based decision-making, facilitates decentralised trust evaluation and provides CTI producers with highly granular sharing of CTI is lacking. Subsequently, in this paper, we propose a blockchain-based CTI sharing framework, called Priv-Share, as a promising solution towards this challenge. In particular, we highlight that the integration of differential sharing, trustless delegation, democratic group managers and incentives as part of Priv-Share ensures that it can satisfy these criteria. The results of an analytical evaluation of the proposed framework using both queuing and game theory demonstrate its ability to provide scalable CTI sharing in

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN:2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May-June 2025 ||

DOI:10.15680/IJARETY.2025.1203042

a trustless manner. Moreover, a quantitative evaluation of an Ethereum proof-of-concept prototype demonstrates that applying the proposed framework within real-world contexts is feasible.

No of users	Input Tx's	Channels	Organizations	Ordering peers	Committing peers	Endorsing peers	Rounds
100	1000	1	2	4	4	4	100
200	2000	2	2	8	8	8	100
300	3000	3	2	12	12	12	100
400	4000	4	2	16	16	16	100
500	5000	5	2	20	20	20	100

Table 1. Configuration parameters.

Block Chain

Blockchain is a shared immutable ledger that facilitates the process of recording transactions and tracking assets across a business network. Anything of value can be tracked and traded on the Blockchain network. A Blockchain is a distributed database, which is shared over a computer network. Blockchain stores information electronically in a digital format to make transactions secure.

Blockchain is a new technology, which is known as Distributed Ledger Technology (DLT). With the help of Blockchain technology, currency as well as anything can be converted into digital format and stored. Actually it is an exchange process, which works on data blocks. In this, one block is connected to another block. These blocks cannot be hacked. Blockchain technology aims to keep documents digitally secure. You can take Google Doc as an example to understand Blockchain technology. When we create a document and share it with a group of people, the document is distributed instead of copied or transferred. But, Blockchain is more complex than Google Doc. Simply put, Blockchain is known as Distributed Ledger Technology, which makes any digital asset immutable and transparent through the use of decentralization.

Smart Contract

A smart contract is a self-executing program that automates the actions required in a blockchain transaction. Once completed, the transactions are trackable and irreversible. The best way to envision a smart contract is to think of a vending machine—when you insert the correct amount of money and push an item's button, the program (the smart contract) activates the machine to dispense your chosen item.

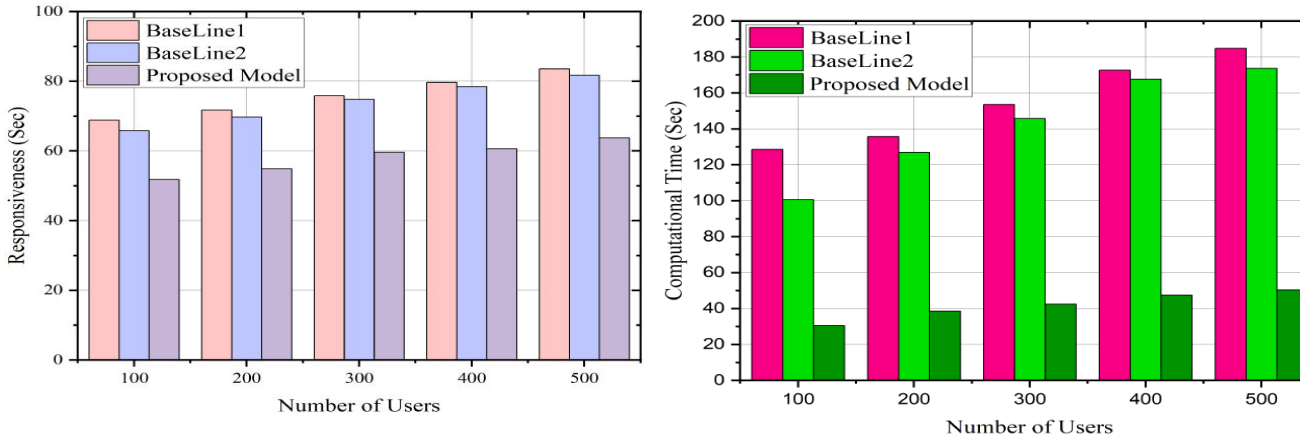

Figure 5. Responsiveness & Computational time.

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN:2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May-June 2025 ||

DOI:10.15680/IJARETY.2025.1203042

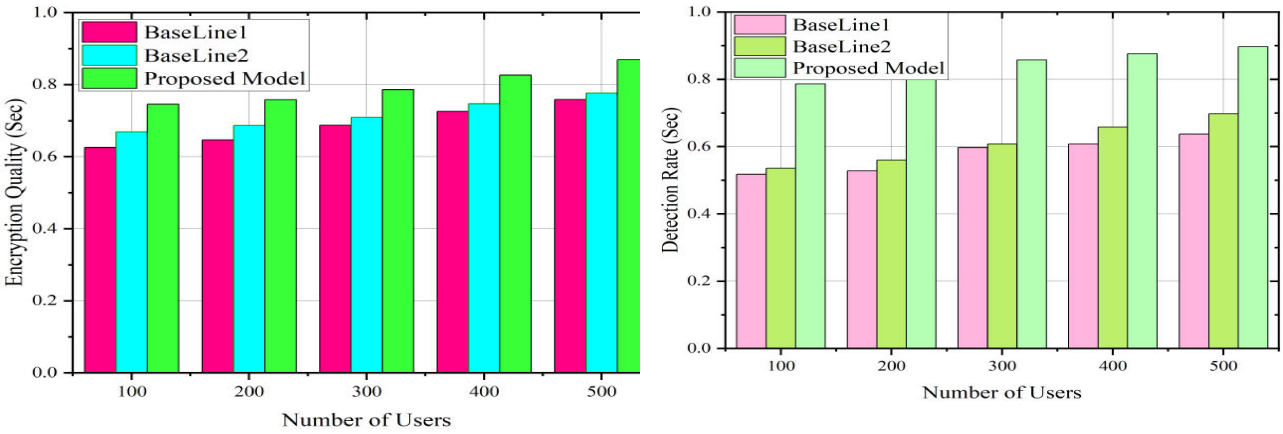

Figure 6. Encryption quality & Detection rate.

Smart contracts permit trusted transactions and agreements to be carried out among disparate, anonymous parties without the need for a central authority, legal system, or external enforcement mechanism. While blockchain technology has come to be thought of primarily as the foundation for Bitcoin, it has evolved far beyond underpinning a virtual currency.

IV.CONCLUSION AND FUTURE WORK

In this paper, Blockchain secures and anonymizes IoT and its applications. Smart city challenges include user security, privacy, bandwidth, anonymity, and scalability. Therefore, this study proposes a blockchain-based SecPrivPreserve system. The presented framework ensures the privacy and safety of the user's data throughout processing. In the Hyperledger Fabric blockchain, information is summarized, and specific features of business transmission are systematized based on the model. Initialization, registration, data protection, authentication, data access control, validation, data sharing and download comprise in SecPrivPreserve framework. Security features include passwords, OTP, encryption, hashing, digital signature, Chebyshev polynomials, and interpolation. Cutting-edge experiments demonstrated that SecPrivPreserve outperformed state-of-the-art systems in responsiveness, processing time, encryption quality, and detection rate. However, the experimentation was carried out through Fabric SDK, and the obtained results show that the proposed framework reduces computational time and responsiveness.

REFERENCES

[1] C. Vanmathi, R. Mangayarkarasi, and R. J. Subalakshmi, ''Real time weather monitoring using Internet of Things,'' in Proc. Int. Conf. Emerg. Trends Inf. Technol. Eng. (ic-ETITE), Feb. 2020, pp. 1–6.
[2] Ravindra Changala, "Sustainable Manufacturing through Predictive Maintenance: A Hybrid Jaya Algorithm and Sea Lion Optimization and RNN Model for Industry 4.0", 2024 8th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), ISSN: 2768-0673, DOI: 10.1109/I-SMAC61858.2024.10714701, October 2024, IEEE Xplore.
[3] Ravindra Changala, "Enhancing Robotic Surgery Precision and Safety Using a Hybrid Autoencoder and Deep Belief Network Approach: Real-Time Feedback and Adaptive Control from Image Data",2024 8th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), ISSN: 2768-0673, DOI: 10.1109/I-SMAC61858.2024.10714701, October 2024, IEEE Xplore.
[4] [2] B. Bryant and H. Saiedian, ''Key challenges in security of IoT devices and securing them with the blockchain technology,'' Secur. Privacy, vol. 5, no. 5, p. e251, Sep. 2022.
[5] Ravindra Changala, "Hybrid AI Approach Combining Decision Trees and SVM for Intelligent Tutoring Systems in STEM Education", 2024 10th International Conference on Advanced Computing and Communication Systems (ICACCS), ISSN: 2575-7288, DOI: 10.1109/ICACCS60874.2024.10717088, October 2024, IEEE Xplore.
[6] F. Al-Turjman, H. Zahmatkesh, and R. Shahroze, ''An overview of security and privacy in smart cities' IoT communications,'' Trans. Emerg. Telecommun. Technol., vol. 33, no. 3, p. e3677, Mar. 2022.

[7] Ravindra Changala, "Sentiment Analysis in Mobile Language Learning Apps Utilizing LSTM-GRU for Enhanced User Engagement and Personalized Feedback", 2024 Third International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT), ISBN:979-8-3503-6908-3, DOI: 10.1109/ICEEICT61591.2024.10718406, October 2024, IEEE Xplore.
[8] Ravindra Changala, "Image Classification Using Optimized Convolution Neural Network", 2024 Parul International Conference on Engineering and Technology (PICET), ISBN:979-8-3503-6974-8, DOI: 10.1109/PICET60765.2024.10716049, October 2024, IEEE Xplore.
[9] The Editors of Encyclopaedia. (Dec. 9, 2023). United Nations Population Fund. Encyclopedia Britannica. Accessed: Jun. 6, 2023.
[10] V. Moustaka, Z. Theodosiou, A. Vakali, and A. Kounoudes, ‘‘Smart cities at risk! Privacy and security borderlines from social networking in cities,’’ in Proc. Companion The Web Conf. Web Conf., 2018, pp. 905–910.
[11] Ravindra Changala, "Sentiment Analysis Optimization Using Hybrid Machine Learning Techniques", 2024 Parul International Conference on Engineering and Technology (PICET), ISBN:979-8-3503-6974-8, DOI: 10.1109/PICET60765.2024.10716049, October 2024, IEEE Xplore.
[12] Ravindra Changala, "Using Generative Adversarial Networks for Anomaly Detection in Network Traffic: Advancements in AI Cybersecurity", 2024 International Conference on Data Science and Network Security (ICDSNS), ISBN:979-8-3503-7311-0, DOI: 10.1109/ICDSNS62112.2024.10690857, October 2024, IEEE Xplore.
[13] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, and W. Ni, ‘‘Anatomy of threats to the Internet of Things,’’ IEEE Commun. Surveys Tuts., vol. 21, no. 2, pp. 1636–1675, 2nd Quart., 2019.
[14] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen, ‘‘Security and privacy in smart city applications: Challenges and solutions,’’ IEEE Commun. Mag., vol. 55, no. 1, pp. 122–129, Jan. 2017.
[15] S. Chaudhary and P. K. Mishra, ‘‘DDoS attacks in industrial IoT: A survey,’’ Comput. Netw., vol. 236, Nov. 2023, Art. no. 110015.
[16] L. Cui, G. Xie, Y. Qu, L. Gao, and Y. Yang, ‘‘Security and privacy in smart cities: Challenges and opportunities,’’ IEEE Access, vol. 6, pp. 46134–46145, 2018.
[17] Ravindra Changala, "Healthcare Data Management Optimization Using LSTM and GAN-Based Predictive Modeling: Towards Effective Health Service Delivery", 2024 International Conference on Data Science and Network Security (ICDSNS), ISBN:979-8-3503-7311-0, DOI: 10.1109/ICDSNS62112.2024.10690857, October 2024, IEEE Xplore.
[18] Ravindra Changala, "Implementing Genetic Algorithms for Optimization in Neuro-Cognitive Rehabilitation Robotics", 2024 International Conference on Cognitive Robotics and Intelligent Systems (ICC - ROBINS), ISBN:979-8-3503-7274-8, DOI: 10.1109/ICC-ROBINS60238.2024.10533965, May 2024, IEEE Xplore.
[20] Z. Xihua and D. S. B. Goyal, ‘‘Security and privacy challenges using IoTblockchain technology in a smart city: Critical analysis,’’ Int. J. Electr. Electron. Res., vol. 10, no. 2, pp. 190–195, Jun. 2022.
[21] P. M. Rao and B. D. Deebak, ‘‘Security and privacy issues in smart cities/industries: Technologies, applications, and challenges,’’ J. Ambient Intell. Humanized Comput., vol. 14, no. 1, pp. 1–37, Feb. 2022.
[22] Ravindra Changala, "Real-Time Anomaly Detection in 5G Networks Through Edge Computing", 2024 Third International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS), ISBN:979-8-3503-6118-6, DOI: 10.1109/INCOS59338.2024.10527501, May 2024, IEEE Xplore.
[23] Ravindra Changala, "Enhancing Quantum Machine Learning Algorithms for Optimized Financial Portfolio Management", 2024 Third International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS), ISBN:979-8-3503-6118-6, DOI: 10.1109/INCOS59338.2024.10527612, May 2024, IEEE Xplore.
[24] Ravindra Changala, "Integration of Machine Learning and Computer Vision to Detect and Prevent the Crime", 2023 International Conference on New Frontiers in Communication, Automation, Management and Security (ICCAMS), ISBN:979-8-3503-1706-0, DOI: 10.1109/ICCAMS60113.2023.10526105, May 2024, IEEE Xplore.
[25] M. Ramaiah, V. Chandrasekaran, V. Ravi, and N. Kumar, ‘‘An intrusion detection system using optimized deep neural network architecture,’’ Trans. Emerg. Telecommun. Technol., vol. 32, no. 4, p. e4221, Apr. 2021.
[26] Ravindra Changala, "Swarm Intelligence for Multi-Robot Coordination in Agricultural Automation", 2024 10th International Conference on Advanced Computing and Communication Systems (ICACCS), ISSN: 2575-7288, DOI: 10.1109/ICACCS60874.2024.10717088, October 2024, IEEE Xplore.
[27] M. Gupta, F. M. Awaysheh, J. Benson, M. Alazab, F. Patwa, and R. Sandhu, ‘‘An attribute-based access control for cloud enabled industrial smart vehicles,’’ IEEE Trans. Ind. Informat., vol. 17, no. 6, pp. 4288–4297, Jun. 2021.

International Journal of Advanced Research in Education and Technology

ISSN: 2394-2975 Impact Factor: 8.152

www.ijarety.in editor.ijarety@gmail.com