



IJRASET

International Journal For Research in
Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** V **Month of publication:** May 2025

DOI: <https://doi.org/10.22214/ijraset.2025.71720>

www.ijraset.com

Call:  08813907089

E-mail ID: ijraset@gmail.com

Design of an Efficient and Secure Smart City Framework Using Blockchain

Bogaraju Archana¹, Malakadi Spandana², Bolli Vijith Kumar³, Mr.CH.Gopi⁴

^{1, 2, 3}Students, ⁴Assistant Professor, Department of Information Technology, Guru Nanak Institutions Technical Campus, Hyderabad, Telangana, 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: SHA256, Blockchain, CryptoGraphic Techniques, Authentication, SmartContract

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, resource-constrained 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 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 SURVEY

1) Title: A review of security vulnerabilities in Industry 4.0 application and the possible solutions using blockchain.

Author: M. Ramaiah, V. Chithanuru, A. Padma, and V. Ravi.

Year: 2023.

Description:

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 cybersecurity 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 solutions using blockchain technologies.

2) Title: VeDB: A software and hardware enabled trusted relational database.

Author: X. Yang, R. Zhang, C. Yue, Y. Liu, B. C. Ooi, Q. Gao, Y. Zhang, and H. Yang,

Year: 2023

Description:

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 Shrub 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 an non-intrusive trusted affiliation by TEE leveraging digests 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 $70\times$ and $3.7\times$ for insertion and verification; and VeDB-Ve-H data lineage verification is $8.5\times$ faster than Ve-S.

3) Title: Private blockchain envisioned access control system for securing industrial IoT-based pervasive edge computing.

Author: S.Saha, B.Bera, A.K.Das, N.Kumar, S.H.Islam, and Y.Park.

Year: 2023

Description:

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 intuitiveness to drive smarter, faster and effective business agreements. IIoT having interconnected machines along 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-PEC IIoT. 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-PEC IIoT 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-PEC IIoT achieves greater security and more functionality features, and requires low costs for communication and computational as compared to other pertinent schemes.

III. METHODOLOGIES

The proposed project aims to develop a blockchain-based framework, SecPrivPreserve, to enhance the security, privacy, and integrity of data in IoT-based smart city applications. As smart cities increasingly rely on IoT devices for monitoring, managing, and improving urban life, ensuring secure and efficient data sharing among these devices becomes crucial. Current centralized systems are vulnerable to security breaches, data tampering, and privacy violations, which compromise the effectiveness of smart city services. The SecPrivPreserve framework addresses these challenges by leveraging blockchain technology to create a decentralized and tamper-proof system for data storage, transmission, and sharing. It integrates various security mechanisms such as OTP-based passwords, encryption, hashing, and QR code-based encryption to safeguard sensitive data and ensure privacy.

The following modules:

- User Interface Design
- MSP
- Authority
- Client
- Upload
- Smart Contract

1) User Interface Design

To connect with server user must give their username and password then only they can able to connect the server. If the user already exists directly can login into the server else user must register their details such as username, password, Email id, City and Country into the server. Database will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter a specific page. It will search the query and display the query.

2) Membership Service Providers (MSP):

Certificate Authorities (CA) are responsible for issuing X.509 certificates to network entities. MSP specifies which CA is permitted to participate in the blockchain network and uses this information to identify which peer nodes belong to which groups. MSP maintains the distributed ledger between organizations and associated systems that the network trusts.

3) Authority

This is the third module in our project where Data owner has all permissions on data like delete, update, and insert on user records play the main part of the project role. Authority login first then it starts with his registration data and store his data inside cloud.

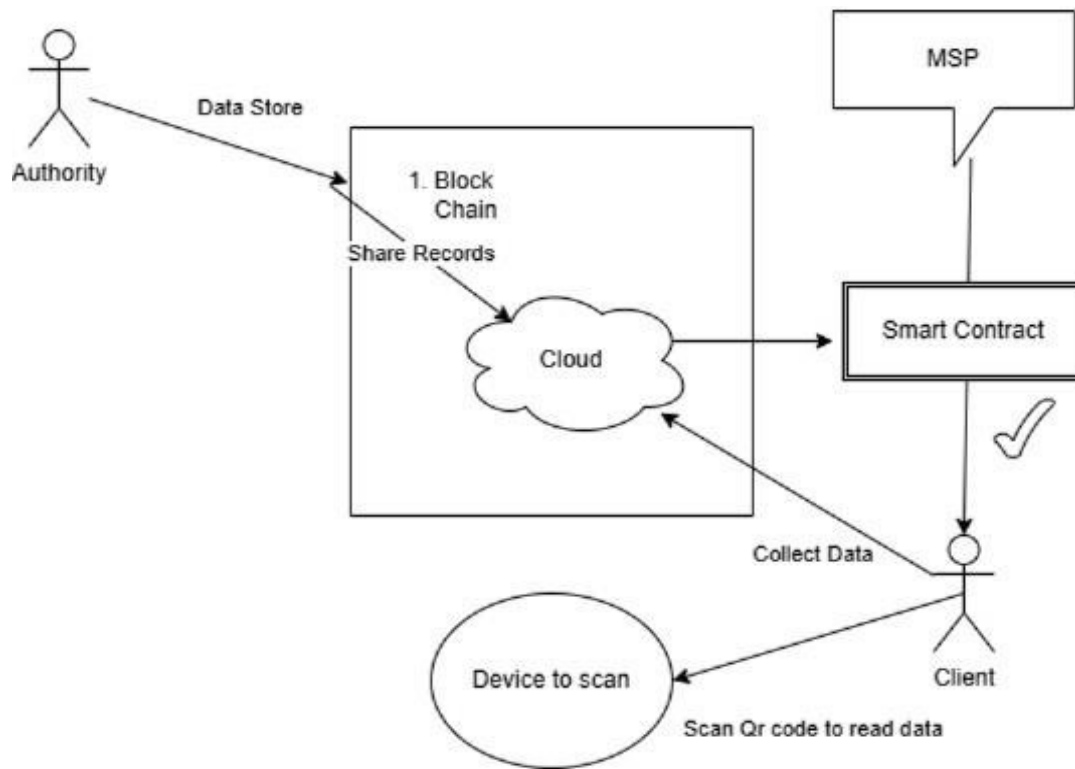
4) *SmartContract*

Smart contracts are typically used to automate the execution of an agreement so that all participants can be immediately certain of the outcome, without any intermediary's involvement or time loss. They can also automate a workflow, triggering the next action when predetermined conditions are met.

5) *Client*

This is the Fifth module in our project where data User plays the main part of the project role. User registers and then logs in to the application, the registration details are stored inside the database. After User Login, he will directly navigate to the User home page and access data by searching with keywords. When data owner uploads data, the data will be encrypted, the encrypted keys will be stored inside the database, and keys will be shredded with a key repository.

IV. SYSTEM ARCHITECTURE



In a blockchain network, various entities collaborate to ensure its proper functioning. The Client (C) collects user data records, while the Authority manages permissions like updating or deleting records. Membership Service Providers (MSP) issue certificates to trusted network participants and maintain the ledger. A Smart Contract (SC) automates digital asset transfers and records transactions on the ledger. Endorsing Peers (EP) validate transaction proposals, and Ordering Peers (OP) organize and add transaction blocks to the ledger. Committing Peers (CP) validate and commit these transactions, ensuring the ledger is up to date. Channels enable communication between organizational peers within the network.

V. TECHNIQUE USED OR ALGORITHM USED

1) *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.

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* ensure 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 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.

2) 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 Docs 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.

3) 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.

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.

VI. CONCLUSION

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] 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.
- [3] 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.
- [4] The Editor of Encyclopaedia. (Dec. 9, 2023). United Nations Population Fund. Encyclopaedia Britannica. Accessed: Jun. 6, 2023.



- [5] 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 WebConf. WebConf., 2018, pp. 905–910.
- [6] 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.
- [7] 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.
- [8] S. Chaudhary and P. K. Mishra, "DDoS attacks in industrial IoT: A survey," Comput. Netw., vol. 236, Nov. 2023, Art. no. 110015.
- [9] 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.
- [10] Z. Xihua and D. S. B. Goyal, "Security and privacy challenges using IoT blockchain technology in a smart city: Critical analysis," Int. J. Electr. Electron. Res., vol. 10, no. 2, pp. 190–195, Jun. 2022.
- [11] P. M. Rao and B. D. Deebak, "Security and privacy issues in smart cities/industries: Technologies, applications, and challenges," J. Ambient Intel. Hum. Comput., vol. 14, no. 1, pp. 1–37, Feb. 2022.
- [12] 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.



10.22214/IJRASET



45.98



IMPACT FACTOR:
7.129



IMPACT FACTOR:
7.429



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089  (24*7 Support on Whatsapp)