DESIGN OF AN EFFICIENT AND SECURE SMART CITY FRAMEWORK USING BLOCKCHAIN

Mubasheera Fatima[1], Dr. C. Berin Jones[2]
[1]PG Scholar, Department of CSE, Shadan Women's College of Engineering and Technology, Hyderabad, mubasheera8101@gmail.com
[2]Professor, Department of CSE, Shadan Women's College of Engineering and Technology
jonesberin@gmail.com

ABSTRACT
One of the main goals of contemporary technology breakthroughs is the development of smart services for smart cities. In order to collect and process data from a variety of sources, mobile scanners are essential. Applications for smart cities highlight how important it is for diverse devices to share data securely. However, some data sharing practices can put data integrity, security, and privacy at risk. One of the main causes of previous security breaches has been the dependence on a centralized repository. Therefore, it is essential for modern apps to ensure safe authentication and the protection of sensitive data. Blockchain is a popular technology that guarantees the confidentiality and integrity of data. This study presents SecPrivPreserve, a cutting-edge blockchain-based architecture intended to improve the security and integrity of data produced by mobile scanners. Initialization, registration, data protection, authentication, access control, validation, data sharing, and safe downloads are some of the stages that the suggested framework uses to secure data. SecPrivPreserve incorporates a number of security-enhancing measures, including hashing, encryption, and authentication methods, to improve confidentiality, privacy, and integrity. This system uses QR codes for secure access and data-sharing keys to further improve security, in contrast to conventional methods that rely on one-time passwords (OTP) for authentication and data sharing. The SecPrivPreserve structure naturally benefits from non-repudiation and tamper-proof records because it is based on a permissioned blockchain. Additionally, data protection methods can improve the security of cryptography.

1. INTRODUCTION

In recent years, every country in the globe has been utilizing smart technology to improve its infrastructure, services, and apps for the benefit of their citizens. In order to enable data transfer between many locations, the Internet of Things (IoT) is essential for connecting physical devices to the internet utilizing various protocols. IoT-based services have become more necessary in the last few decades in a number of industries, including manufacturing, healthcare, financial services, energy transfer, traffic and weather monitoring, and more. The use of IoT devices is predicted to surpass $1.4 trillion by 2027 because to its portability and low power consumption. Numerous nations make significant financial investments in smart city projects. For example, China is working on over 220 projects to make cities smarter and raise the standard of living for its people. Intelligent city-related technology help urban municipalities run their daily activities more efficiently. The three primary features of a smart city, according to IBM, are instrumented (sensors, actuators), linked (devices transmitting input), and intelligent (improving the quality of life for people). According to recent observations, smart cities have significantly improved urban residents' amenities and quality of life. Over half of the world's population resides in cities, per a report from the United Nations Population Fund. Both academia and industry have taken notice of the smart city since it has greatly reduced the logistical issues associated with to purchasing services. To raise the standard of living for their residents, a number of towns throughout the world have started developing their own smart city plans. Smart surroundings and IoT are now interchangeable terms. Because IoT technology can sense anything in the real world, it is useful in public safety, healthcare, transportation, traffic systems, smart buildings, and smart agriculture. Despite its many advantages, IoT devices are susceptible to security and privacy breaches because of their centralized repository, resource constraints, and uneven protocol standards. Because of the weaknesses in smart city applications, people may be at risk for privacy and security issues in a smart environment. The decision-making system may be compromised, for example, if malevolent attackers fabricate data to carry out their nefarious goal. Furthermore, in an effort to lower the quality of intelligent city services, these malevolent attackers employ a variety of tactics to stop legitimate customers from using the service, including denial-of-service (DoS) attacks, transmission disruptions, and interference with sensing and control. Additionally, the complexity of the hazards associated with smart city applications increases with the number of linked devices or software, especially when it comes to privacy. Regretfully, the majority of security measures (such as encryption and

authentication) are not enough to shield smart city apps from the emerging, ever-changing dangers. The gadgets' limited computational capacity would make it impossible to implement intricate processes. Therefore, it makes sense that a straightforward framework that takes into account basic cryptographic approaches would be a suitable response to the variety and dynamic nature of the Internet of Things.

Data owners and providers face serious risks when data breaches happen during data storage, transport, and exchange. There are rules in place to guard against potential damage from target data nodes to the system and the data source. Therefore, both the source and target nodes must adhere to the rules and laws of their respective regions when conducting data transactions. The foundation of smart cities is the integration of sensors and smart technology, which enables individuals and institutions to access, process, and use data via their smart devices. However, privacy issues are brought up by the use of data in smart cities, including the possibility of sensitive data being compromised by data poisoning attacks. Important information may be altered as a result of these attacks, which could then cause communication problems within smart entities. Smart city IoT networks are especially vulnerable to cyberattacks that jeopardize the systems' availability, confidentiality, and data integrity. Smart cities must put strong security measures in place to guard their assets against cyberattacks (Distributed Denial of Service (DDoS), DoS, Man-in-the-Middle, and ransomware) in order to reduce these risks. The necessity of sufficient privacy and security protections in digital towns is highlighted by the frequency and severity of these attacks.To provide confidentiality and safety for apps intended for smart city applications, researchers have created a variety of data-securing systems. The data integrity and privacy concerns of smart apps have not been addressed by previous centralized cloud-based data-sharing frameworks. Blockchain-based solutions, on the other hand, offer further advancement in addressing privacy concerns. First, client data is divided into different groups according to similarity labels using sensor data gathered by a detection algorithm. With a specified detection algorithm, it has a certain kind of control on community data. Nevertheless, data protection has not been covered by this framework.

SCOPE OF THE PROJECT

In order to correctly store and authenticate client data and guarantee the numerous security benefits of privacy and integrity, the new architecture is divided into seven distinct phases. In order to start the request, each participant's identification number was generated using a random number string and hashed using SHA256 during the startup phase. During the registration step, various peer types use passwords created using the current time and hashed random number (OTP) to complete the enrollment process. The client data is encrypted during the data protection phase using the AES technique (128-bit key length). In the data protection phase, Chebyshev polynomials and interpolation are also used to boost the level of confidentiality. Using a digital signature and hashing, the MSP verifies the clients' data. Hashed passwords are used to prevent data manipulation and to facilitate data access control. Data sharing uses AES and Chebyshev polynomials to download the data for verification reasons.

OBJECTIVE

The literature shows that because of the blockchain's useful qualities, there is a significant need to integrate it with other business logic. The fact that a blockchain is a peer-to-peer network devoid of a central authority is its most crucial feature. Many researchers presented alternative frameworks employing blockchain technologies to enhance the security aspects of smart city applications. The most notable feature of distributed ledger technology is its immutability, which is drawing more interest in the creation of reliable data-sharing methods for smart cities.

One of the primary goals of apps for smart environments has been to ensure privacy. One of the initiatives to establish privacy in smart cities is privySharing. To facilitate effective data interchange and security, the decentralized network is divided into multiple channels for the registered organizations. Artificially intelligent agreements are used to keep the data.

PROBLEM STATEMENT

To build trust amongst the different Industrial IoT (IIoT) components, a centralized cloud-based platform for cross-domain data sharing that integrates blockchain technology to satisfy industrial requirements is required. Consumers are storing their data on the blockchain to lessen the drawbacks of conventional cloud storage. By informing the blockchain of any harmful activity attempted in centralized storage, this makes it possible to detect it. The Ephemeral Elliptic Curve Diffie-Hellman method improves security characteristics in accordance with industry standards. Finding a balance between security precautions and budgetary concerns is essential. However, more research is required to determine the framework's capacity to manage massive amounts of data.

EXISTING SYSTEM

To build trust between the many Industrial IoT components, a centralized cloud-based platform for cross-domain data sharing that integrates blockchain technology to satisfy industrial needs is required. Data owners are putting their data on the blockchain in order to lessen the drawbacks of conventional cloud storage. By informing the blockchain of any harmful activity attempted in centralized storage, this makes it possible to detect it. IoT devices in smart cities nowadays mainly depend on centralized repositories for managing and storing data. These repositories are prime targets for assaults because they hold enormous volumes of private information gathered from numerous devices. To protect data, the current systems frequently rely on conventional security measures like hashing, passwords, and simple encryption. Furthermore, centralized systems are susceptible to problems like data breaches, tampering, and single points of failure, which jeopardize security and undermine confidence in apps for the IoT.

Existing System Disadvantages

- Existing security measures, including simple encryption and authentication
- Frequently insufficient to handle the new and dynamic risks that arise as IoT devices are continuously added to the network.
- These issues include data confidentiality, limited scalability, and inadequate privacy protection.

PROPOSED SYSTEM

In order to provide data protection for smart cities, we presented in this paper an effective and safe privacy-preserving framework called SecPrivPreserve that uses the Hyperledger Fabric blockchain. The framework resolves the shortcomings of centralized systems by utilizing the advantages of permissioned blockchain technology to guarantee secure data sharing amongst IoT devices, non-repudiation, and tamper-proof data storage. Throughout the data lifecycle, from initialization and registration to accessibility control, validation, and sharing, it integrates a number of security measures, such as hashing, encryption, QR code-based encryption, and OTP-based passwords. Quantitative measures are used to compare the tested findings with established frameworks in the candidate domain in order to demonstrate its effectiveness.

Proposed System Advantages

- Effective Cryptographic Methods.
- Improved Cyberattack Protection.
- Several security stages, such as data protection, authentication, access control, validation, and data sharing, to offer a comprehensive security solution for Internet of Things applications in smart cities.

2. RELATED WORKS

Industry 4.0 is a technological endeavor designed to increase the creative manufacturing sectors' task efficiency. Trending technologies like the Internet of Things, Industrial Internet of Things, Artificial Intelligence, and Big Data analytics are all part of Industry 4.0, which also presents obstacles as it adapts to the task. Cybersecurity attacks are not an exception to the rule for popular smart technologies. Strong and intelligent defenses are necessary for the networked devices to enable automation and stop the hacking that could be expected from the anonymous entity. Therefore, in order to avoid safety hazards, it is crucial to have a thorough grasp of the numerous safety concerns of the industrial revolution. This chapter aims to draw attention to the potential security flaws that are expected to arise from the system's essential components as well as the potential blockchain-based security fix. **[1]**

In recent years, blockchain-like ledger databases have become a more effective substitute for permissioned blockchains. Traditional ledger databases have performance issues since they primarily rely on authenticated structures like transparency logs and the Merkle tree to enable auditability. We design VeDB, a high-performance verifiable software (Ve-S) and hardware (Ve-H) enabled DBMS with rigorous auditability for greater user options and a wider range of applications, in contrast to traditional ledger DBMSs. We develop a new verified Shrubs array (VSA) in Ve-S that uses two-layer ordinals (serial numbers) and performs better than traditional Merkle tree-based models since it uses less CPU and I/O. Through its effective, reliable timestamp range authentication approach and fine-grained client-side data verification— features that are absent from modern relational ledger databases—it permits rigorous auditability. Using digest signing, monotonic counters, and trusted timestamps in VeDB, we provide a non-intrusive trusted affiliation by TEE in Ve-H that facilitates lineage and data notarization applications. According to the experimental results, VeDB Ve-H data lineage verification is 8.5× faster than Ve-S, and VeDB-VSA performs better than Merkle tree-based authenticated data structures (ADS) up to 70× and 3.7× for insertion and verification.**[2]**

With the use of IoT smart devices, gateway nodes, and edge devices, the Industrial Internet of Things (IIoT) may link people, machines, and analytics to generate significant insights that facilitate quicker, more intelligent, and more successful business deals. Knowledge can be monitored, collected, shared, and

analyzed by IIoT devices and equipment that are connected. An attacker can readily alter the data since the communication between the entities in the IIoT ecosystem occurs in an insecure manner (for example, wireless communications and the Internet). Furthermore, an intruder can launch impersonation and other assaults by physically stealing IoT smart devices. In this work, we design PBACS-PECIIoT, a new private blockchain-envisioned access control scheme for Pervasive Edge Computing (PEC) in an IIoT environment, to address such important challenges. Since the data is extremely safe and sensitive, we take into consideration the private ledger that contains the transactions and enrollment data of the IIoT-related companies. The use of blockchain technology, which offers immutability, transparency, and decentralization in addition to defense against a variety of potential threats, greatly enhances the security of PBACS-PECIIoT. A thorough comparison shows that, in comparison to other relevant systems, PBACS_PECIIoT provides greater privacy, added features, and lower transport and computing costs. **[3]**

Because it encourages users to provide high-quality knowledge, incentives are crucial for learning discovery. BC technology has been extensively utilized in incentive systems to offer transparency. At the moment, creating blockchain-based incentive programs poses multiple difficulties, including concealment, consistency, quick approval, as well as awareness. In this work, we create FRUIT, a blockchain-based incentive scheme that is efficient, privacy preserving, and quality-aware. FRUIT accomplishes secrecy, dependability, efficient processing, and quality awareness throughout the method via clever agreements that are well designed. In particular, we combine matrix decomposition with proxy re-encryption and a privacy-preserving job allocation based on the polynomial fitting function and hashing algorithm to create a revolutionary lightweight encryption technique. Then, in order to safely compute the data quality and truthful expertise, we use our suggested minimal cryptography and job allocation to create an effective and confidential discovery protocol. We employ the Dirichlet distribution to implement the automatic reputation prediction based on the data quality by implementing the reputation management on the blockchain in order to guarantee user trust in the incentive scheme. Additionally, we implement payment administration on the blockchain, enabling the incentive program to routinely compensate individuals according to the quality of the data. We show through a thorough security study that task and private information are effectively maintained during the entire procedure. Numerous trials on real-world data sets and theories show that FRUIT performs rather well in terms of compute cost, communication overhead, and gas consumption. **[4]**

The Internet of Things (IoT) is emerging as an intriguing innovation to understand sustainable smart cities, thanks to the growth of devices with sensors and the explosion of low-cost electronic circuits. To improve the level of life for their residents, smart cities can implement a number of clever usage, such as 4.0 manufacturing, smart banking, and smart transportation. But one of the main issues with a smart city is security. Users can only gain from these new IoT-based smart infrastructure and applications provided essential private and secure aspects are ensured. Therefore, a Blockchain-enabled Privacy-Preserving Access Control System (BPACS) for IoT data in a smart city setting has been proposed in this work. In order to create a dependable and safe input-sharing policy across several data sources, this study uses chain techniques. IoT info is encoded and subsequently validated on distributed ledgers. Additionally, this study builds a safe Support Vector Machine (SVM) and Principle Component Analysis (PCA) training method and designs protected building blocks, such as secure contrast and secure cubic multiplications, by keeping cryptosystems. The proposed approach ensures the anonymity of delicate information for all data providers and the use of the SVM and PCA parameter sets for data analysts, as demonstrated by hard security analysis. **[5]**

3. METHODOLOGY

Every user of apps for intelligent communities would demand that proprietary and sensitive data collected by various devices not be made public. Designing a refined blockchain system with the goal of ensuring such confidence is always commendable in order to build trust. The flow of the suggested paradigm for creating an effective privacy-preserving method is explained in detail in this section. Strong authentication is necessary for smart city-based applications to implement privacy and stop data leaks. Therefore, in addition to the built-in security measures, an improvised blockchain construction called SecPrivPreserve is greatly needed for the current situation. Initialization, registration, data protection, authentication, data access control, validation, data sharing, and download are among the phases that are taken into account by the framework that is being provided.

MODULES EXPLANATION AND DIAGRAM

User Interface Design: Users must enter their username and password in order to connect to the server; only then may they do so. If the user has already left, they can log in directly; if not, they must

register their information on the server, including their username, password, email address, city, and country. To maintain the upload and download rate, the database will generate an account for every user. The user ID will be assigned to the name. Usually, logging in allows you to access a certain page. The query will be searched and displayed.

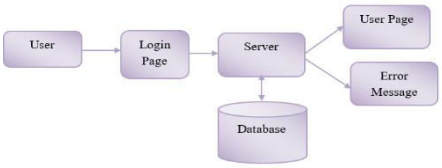


Fig 1. User Interface Design

Membership Service Providers (MSP):

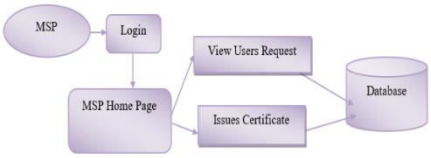


Fig 2. Membership Service Provider

X.509 certificates are issued to network entities by Certificate Authorities (CA). MSP uses this information to determine which peer nodes are members of certain groups and specifies which CA is allowed to join in the blockchain network. The network's trusted distributed ledger between organizations and related systems is kept up to date by MSP.

Authority: The primary function of the project role is played by the third module, where the data owner has complete control over data, including the ability to add, edit, and remove user records. After logging in with authority, his registration information is stored in the cloud.

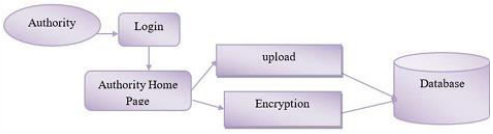


Fig 3. Authority

Smart Contract: Usually, smart contracts are used to automate the implementation of an agreement so that everyone involved can know the result right away, without the need for a middleman or wasting time. They can also automate a workflow, so that when certain conditions are satisfied, the next step is triggered.

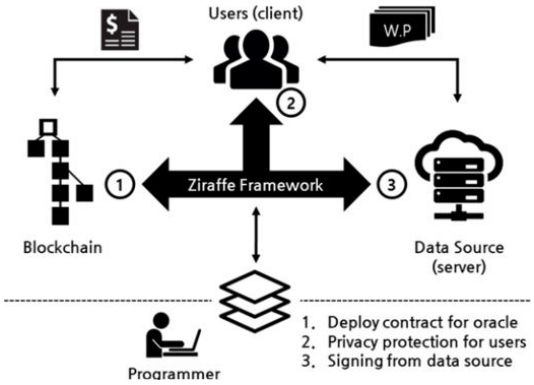


Fig 4. Smart Contract

Client: The data user is the primary project role in this fifth module of our project. The user's registration information is saved in a database after they register and log in to the program. Following user login, he will go straight to the user's home page and use keywords to access data. The data will be encrypted when the owner uploads it, and the encrypted keys will be kept in the database and destroyed using a key repository.

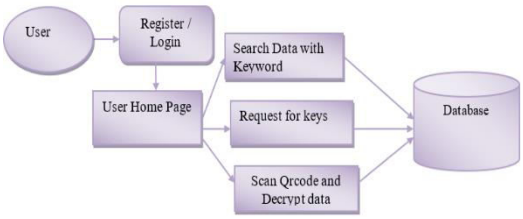


Fig 5. Client

4. TECHNIQUE USED OR ALGORITHM USED

SecPrivPreserve framework

This section provides the outcomes of the blockchain and smart contract-based simulated SecPrivPreserve system. The implementation is done on a system that has an Intel i7 processor, 16 GB of RAM, Ubuntu 20.4 LTS OS, and the SecPrivPreserv framework is developed using the Fabric SDK. The Fabric SDK configuration details. We took into account criteria like calculation time, encryption quality, detection rate, and responsiveness in order to assess the efficacy of the suggested model. The efficacy of the suggested SecPrivPreserve framework is compared with the traditional blockchain-based methods BaseLine 1 and BaseLine 2 model is primarily concerned with the validation process and controlling access to data from various sources. These BaseLine models are developed based on the classical blockchain approach and the phases are explained in the proposed methodology. The following metrics are considered for experimental evaluation with the proposed model, and these metrics are compared with

BaseLine models. Computational Time: It is the runtime, or the entire amount of time the system needs to complete the authentication process, measured using computational cost. Detection Rate: It is measured as the proportion of the total number of users who have been verified as real to all users.

Block Chain

Blockchain is a shared unchangeable ledger that makes it easier to track assets and record transactions inside a company network. The Blockchain network allows for the tracking and trading of anything of value. A distributed database that is shared via a computer network is called a blockchain. Blockchain makes transactions safe by storing data in an electronic manner.

Distributed Ledger Technology (DLT), or blockchain, is a relatively young technology. Blockchain technology makes it possible to transform and store anything, including currency, in a digital format. In reality, it is a data block-based interchange procedure. One block is joined to another in this way. It is impossible to hack these blocks. The goal of blockchain technology is to protect digital documents. You can learn about Blockchain technology by using Google Docs as an example. A document is distributed rather than copied or transferred when it is created and shared among a group of people. Blockchain, however, is more complicated than Google Docs.

Blockchain, or Distributed Ledger Technology, is a technology that uses decentralization to make any digital asset visible and unchangeable.

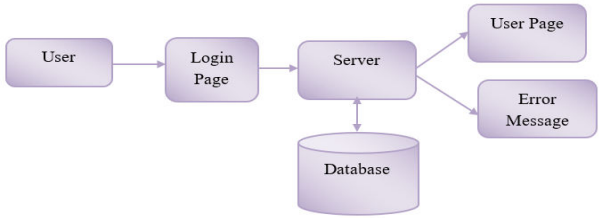
Smart Contract

A self-executing program that automates the steps necessary for a blockchain transaction is called a smart contract. The transactions are irreversible and trackable after they are finished. A smart contract is best pictured as a vending machine, where the program (the smart contract) activates the machine to dispense the item of your choice when you insert the appropriate amount of money and press the button for that item.

Smart contracts eliminate the requirement for a centralized authority, legal system, or external enforcement mechanism by enabling trusted transactions and agreements to be carried out among many, anonymous parties. Blockchain technology has developed far beyond serving as the basis for a virtual currency, even though it is now largely recognized as the technology behind Bitcoin.

5. DATA FLOW DIAGRAM

Level 0



Level 1

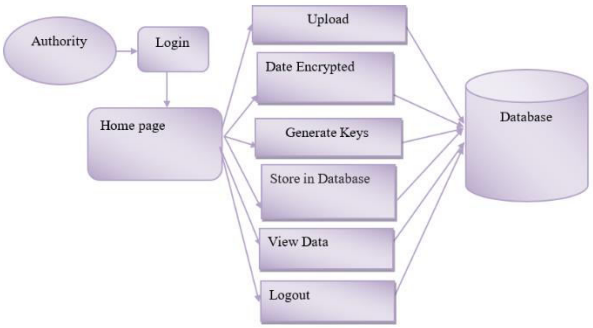


Fig 6. Data Flow Diagram

6. SYSTEM ARCHITECTURE

Several organizations work together to guarantee the correct operation of a blockchain network. While the Authority controls rights like editing or deleting information, the Client (C) gathers user data records. The ledger is kept up to date by Membership Service Providers (MSP), who also grant certificates to reliable network users. A Smart Contract (SC) logs transactions on the ledger and automates the transfer of digital assets. Ordering Peers (OP) arrange and append transaction blocks to the ledger, while Endorsing Peers (EP) verify transaction proposals. To keep the ledger current, Committing Peers (CP) verify and commit these transactions. Communication between organizational peers within the network is made possible by channels.

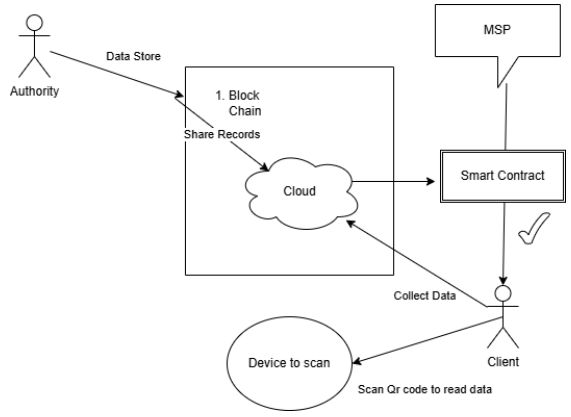


Fig 7. System Architecture

7. RESULTS

The proposed SecPrivPreserve blockchain-based framework achieves better performance and stronger security than conventional centralized repositories and RSA-based smart city systems.Traditional RSA systems were useful but suffered from issues such as large key sizes, slow encryption/decryption, higher power consumption, and weak real-time performance. These drawbacks made them less suitable for IoT-based smart city applications where speed, efficiency, and security are critical.To overcome these challenges, SecPrivPreserve addresses these issues by integrating SHA-256 hashing and AES-128 encryption along with smart contracts and QR-based key management. This combination provides lightweight, faster, and tamper-proof data handling, ensuring secure communication among IoT devices in real-time.

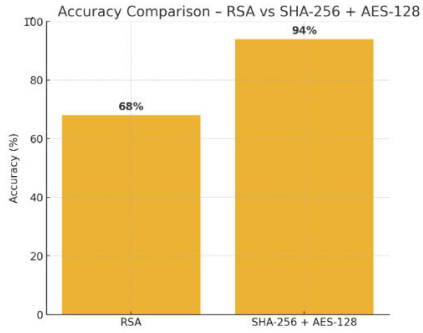


Fig 8. Accuracy Comparison between RSA and SHA 256 + AES 128

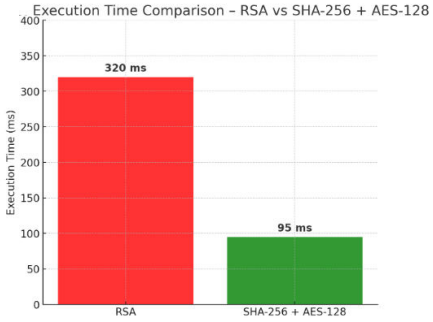


Fig 9. Execution Time Comparison

The results shown in Figures 8 and 9 confirm that the proposed system works as intended. Its accuracy of 94% is noticeably greater than the RSA-based system's 68%. Furthermore, the proposed framework drastically cuts down on execution time; it completes encryption and validation in 95 ms as opposed to 320 ms for RSA. These results clearly show that the SecPrivPreserve method is more efficient, faster, and reliable than standard RSA-based systems, making it highly suitable for real-world smart city applications.

8. FUTURE ENHANCEMENT

In addition, when compared to traditional BaseLine models, it improves the encryption quality and detection rate. By implementing the necessary modifications in the initialization and registration stage, we will assess the candidate SecPrivPreserve's suitability for more smart service applications in the future. It has not yet been determined whether the work described can be applied to smart grids and smart vehicle networks. Leveraging fog/cloud computing to improve the scalability issue and security merits is another potential improvement. The performance of the data-driven model following the implementation of the works that were given was examined.

9. CONCLUSION

This paper discusses how blockchain protects and anonymizes the Internet of Things and its uses. User security, privacy, bandwidth, anonymity, and scalability are among the issues facing smart cities. Thus, a blockchain-based SecPrivPreserve system is suggested in this study. The framework that is being described guarantees the confidentiality and security of user data throughout processing. Information is condensed and particular business transmission aspects are systematized using the Hyperledger Fabric blockchain platform. The SecPrivPreserve framework includes initialization, registration, data protection, authentication, data access control, validation, data sharing, and download. Passwords, OTP, QR-code based encryption, hashing, smart contract, digital signatures, Chebyshev polynomials, and interpolation are examples of security features. Advanced tests showed that SecPrivPreserve performed better than the most advanced systems in terms of detection rate, processing time, encryption quality, and responsiveness. However, the Fabric SDK was used for the experiment, and the findings indicate that the suggested framework decreases responsiveness and processing time.

10. REFERENCE

[1] M. Ramaiah, V. Chithanuru, A. Padma, and V. Ravi, “A review of security vulnerabilities in Industry 4.0 application and the possible solutions using blockchain” 2023.

[2] 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”2023.

[3] S. Saha, B. Bera, A. K. Das, N. Kumar, S. H. Islam, and Y. Park, “Private blockchain envisioned access control system for securing industrial IoT-based pervasive edge computing” 2023.

[4] 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"2022.
[5] P. M. Kumar, B. Rawal, and J. Gao, " Blockchain-enabled privacy preserving of IoT data for sustainable smart cities using machine learning" 2022.
[6] 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.
[7] 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.
[8] 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.
[9] 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.
[10] 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.
[11] 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.
[12] S. Chaudhary and P. K. Mishra, "DDoS attacks in industrial IoT: A survey," Comput. Netw., vol. 236, Nov. 2023, Art. no. 110015.
[13] 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.
[14] 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.
[15] 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.
[16] 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.
[17] 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. [18] M. Ramaiah, V. Chithanuru, A. Padma, and V. Ravi, "A review of security vulnerabilities in Industry 4.0 application and the possible solutions using blockchain," in Cyber Security
Applications for Industry 4.0. London, U.K.: Chapman & Hall, 2023, pp. 63–95.
[19] C.-L. Chen, J. Yang, W.-J. Tsaur, W. Weng, C.-M. Wu, and X. Wei, "Enterprise data sharing with privacy-preserved based on hyperledger fabric blockchain in IIoT's application," Sensors, vol. 22, no. 3, p. 1146, 2022.
[20] U. Khalil, O. A. Malik, and S. Hussain, "A blockchain footprint for authentication of IoT-enabled smart devices in smart cities: State-of-the-art advancements, challenges and future research directions," IEEE Access, vol. 10, pp. 76805–76823, 2022.
[21] N. Deepa, Q.-V. Pham, D. C. Nguyen, S. Bhattacharya, B. Prabadevi, T. R. Gadekallu, P. K. R. Maddikunta, F. Fang, and P. N. Pathirana, "A survey on blockchain for big data: Approaches, opportunities, and future directions," Future Gener. Comput. Syst., vol. 131, pp. 209–226, Jun. 2022.
[22] C. Li, M. Dong, X. Xin, J. Li, X.-B. Chen, and K. Ota, "Efficient privacy preserving in IoMT with blockchain and lightweight secret sharing," IEEE Internet Things J., vol. 10, no. 24, pp. 22051–22064, Dec. 2023
[23] H. Honar Pajooh, M. Rashid, F. Alam, and S. Demidenko, "Hyperledger fabric blockchain for securing the edge Internet of Things," Sensors, vol. 21, no. 2, p. 359, Jan. 2021.
[24] N. K. Tyagi and M. Goyal, "Blockchain-based smart contract for issuance of country of origin certificate for Indian customs exports clearance," Concurrency Comput., Pract. Exp., vol. 35, no. 16, p. e6249, Jul. 2023.
[25] A. Padma and R. Mangayarkarasi, "Detecting security breaches on smart contracts through techniques and tools a brief review: Applications and challenges," in Proc. Int. Conf. Inf. Manage. Eng. Singapore: Springer, 2022, pp. 361–369.
[26] P. Sharma, S. Namasudra, N. Chilamkurti, B.-G. Kim, and R. G. Crespo, "Blockchain-based privacy preservation for IoT-enabled healthcare system," ACM Trans. Sensor Netw., vol. 19, no. 3, pp. 1–17, 2023
[27] M. Tahir, M. Sardaraz, S. Muhammad, and M. S. Khan, "A lightweight authentication and authorization framework for blockchain-enabled IoT network in health-informatics," Sustainability, vol. 12, no. 17, p. 6960, Aug. 2020.
[28] N. B. Truong, K. Sun, G. M. Lee, and Y. Guo, "GDPR-compliant personal data management: A

blockchain-based solution," IEEE Trans. Inf. Forensics Security, vol. 15, pp. 1746–1761, 2019.
[29] J. Chi, Y. Li, J. Huang, J. Liu, Y. Jin, C. Chen, and T. Qiu, "A secure and efficient data sharing scheme based on blockchain in industrial Internet of Things," J. Netw. Comput. Appl., vol. 167, Oct. 2020, Art. no. 102710.
[30] P. Singh, M. Masud, M. S. Hossain, and A. Kaur, "Cross-domain secure data sharing using blockchain for industrial IoT," J. Parallel Distrib. Comput., vol. 156, pp. 176–184, Oct. 2021