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)

4-2975 | 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.2025.1203054

Blockchain-Powered Smart City Framework with Enhanced Privacy and Security

G. Sirisha[1], Talla Anvesh[2], Tallapaka Bhavana[3], Thammadaveni Siddesh[4]

Assistant Professor, Department of CSE, Guru Nanak Institute of Technology, Hyderabad, Telangana, India[1]

Student, Department of CSE, Guru Nanak Institute of Technology, Hyderabad, Telangana, India[2,3,4]

ABSTRACT: With today's technological breakthroughs, creating smart services for smart cities has become a top priority. In these settings, mobile scanners are essential for gathering and analysing data from several sources. Nonetheless, there are still dangers to data integrity, security, and privacy when sharing data securely across diverse devices. Security lapses have frequently occurred in traditional systems that depend on centralised repositories. Blockchain technology has become a dependable remedy for this, providing improved data security and integrity.In this paper, we provide SecPrivPreserve, a new blockchain-based framework for protecting data produced by mobile scanners in applications for smart cities. Initialisation, registration, data protection, authentication, access control, validation, data sharing, and secure downloads are some of the structured phases that make up the framework's operation. To preserve secrecy, privacy, and integrity, it incorporates strong processes like hashing, encryption, and sophisticated authentication systems.In contrast to traditional methods that rely on one-time passwords (OTP) for data sharing and authentication, SecPrivPreserve uses secure data sharing keys and QR codes to provide even more protection. The framework, which is based on a permissioned blockchain, has non-repudiation, traceability, and tamper-proof records. Additionally, it ensures safe, effective, and dependable data management in smart city ecosystems by fortifying cryptographic security using sophisticated data protection measures.

KEYWORDS: Homomorphic encryption, secure data sharing, QR code authentication, data integrity, differential privacy, mobile scanners, access control, smart contracts, tamper-proof records, blockchain, smart cities, IoT data security, privacy-preserving framework, secPrivPreserve, permissioned blockchain, and mobile scanners.

I. INTRODUCTION

In order to raise urban living conditions through smart city projects, countries all over the world have embraced smart technologies more and more in recent years. Connecting physical objects and facilitating smooth data flow across a variety of applications, including public safety, healthcare, traffic management, and smart buildings, are critical functions of the Internet of Things (IoT). Ensuring the security, privacy, and integrity of the enormous volume of data transferred among heterogeneous devices has become a critical concern as IoT services are predicted to expand tremendously. Cyberattacks have shown that traditional centralised repositories for data storage are susceptible to security lapses and data manipulation.Smart city settings are especially vulnerable to advanced threats including data poisoning, denial-of-service (DoS) assaults, and data falsification, which can impair critical services and compromise decision-making systems. Current security techniques, such as password-based authentication and simple encryption, frequently fail to meet the ever-changing security requirements of IoT networks. This project suggests SecPrivPreserve, a decentralised architecture driven by blockchain technology that guarantees safe, authenticated data sharing between IoT devices and tamper-proof data storage in order to get around these restrictions. The framework improves total data security, integrity, and availability by combining multi-phase data validation procedures, advanced cryptographic approaches, and QR code-based authentication. This results in a strong and dependable solution for contemporary smart city applications.

II. LITERATURE REVIEW

Blockchain was suggested by **M. Ramaiah et al. (2023)** as a remedy for security flaws in Industry 4.0 applications. IoT, AI, IoT, and Big Data are all integrated in Industry 4.0, which leaves smart industries open to cyberattacks. Strong, intelligent security measures are necessary for interconnected devices to withstand intrusions from anonymous threats. The study examines how blockchain's immutability, decentralisation, and transparent record-keeping can help mitigate the security threats posed by Industry 4.0's key technologies. Their research highlights the necessity of more thorough comprehension and cutting-edge, blockchain-enabled security measures to protect industrial systems from hostile breaches and changing cyberthreats.

4-2975 | 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.2025.1203054

VeDB, a reliable relational database that combines hardware and software for improved auditability, was proposed by the **X. Yang et al. in 2023**. Performance problems plague traditional blockchain-based ledger databases that use Merkle trees. VeDB offers enhanced CPU and I/O efficiency with its new Verifiable Shrubs Array (VSA), which has two-layer serial numbers. Client-side data verification and strict timestamp range authentication are supported. Additionally, lineage applications and safe data notarisation are made possible by VeDB's Trusted Execution Environment (TEE). For decentralised applications needing strict data integrity, audit trails, and privacy in enterprise settings, the framework guarantees high-performance, reliable data management**.**

A private blockchain-based access control framework for industrial IoT contexts, PBACS-PECIIoT, was created by the **S. Saha et al. in 2023**. In IIoT ecosystems, edge devices and networked equipment exchange private information via unsecure channels. They are therefore vulnerable to theft, impersonation, and data tampering. PBACS-PECIIoT uses a private blockchain to safeguard registration credentials and transaction records, guaranteeing decentralisation, confidentiality, and immutability. The system maintains economical communication and computation overhead while protecting against significant cyberattacks. According to their comparative investigation, PBACS-PECIIoT is a dependable solution for widespread, secure industrial edge computing infrastructures because it performs better in security characteristics than current schemes**.**

FRUIT, a blockchain-based, privacy-preserving, quality-conscious incentive program, was presented by **C. Zhang et al. in 2022.** FRUIT incorporates lightweight encryption through matrix decomposition, proxy re-encryption, and privacy-preserving task allocation, and is designed for transparent, safe knowledge discovery procedures. It protects user privacy while guaranteeing safe data quality computation. Based on the quality of the data, a reputation system based on the Dirichlet distribution forecasts participant reliability. Contributors receive appropriate incentives from blockchain-based payment management. Comprehensive security evaluations attested to the protection of privacy throughout data processing. FRUIT's efficiency, dependability, and low petrol consumption were proven by theoretical and practical assessments on real-world datasets, establishing it as a scalable blockchain incentive system.

BPACS, a Blockchain-enabled Privacy-Preserving Access Control System for IoT data in smart cities, was suggested by **P. M. Kumar et al. in 2022.** Making sure data sharing is safe, confidential, and dependable is essential for smart infrastructure that depends on IoT devices. IoT data is encrypted by BPACS and validated on decentralised ledgers. Additionally, the framework uses sophisticated cryptosystems to build secure operations like comparison and polynomial multiplication. Furthermore, for data analytics, BPACS incorporates the Principal Component Analysis (PCA) and Support Vector Machine (SVM) training methods. Security assessments verified that the framework supports safe, effective, decentralised smart city data management while successfully protecting the privacy of sensitive data.

III. EXISTING SYSTEM

IoT devices in smart cities nowadays mainly depend on centralised 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. These systems, however, have difficulties protecting privacy across heterogeneous devices, limiting unwanted access, and preserving data integrity. Furthermore, centralised systems are susceptible to problems like data breaches, tampering, and single points of failure, which jeopardise security and undermine confidence in IoT applications.

Existing System Disadvantages:

Data Confidentiality.

Limited Scalability.

Insufficient Privacy Protection.

Existing protection methods, such as basic encryption and authentication, are often insufficient to address the new and dynamic threats that emerge as IoT devices are constantly added to the network**.**

Proposed System

To improve the security, privacy, and integrity of IoT data in smart cities, the proposed SecPrivPreserve architecture offers a decentralised, blockchain-based method. The framework resolves the shortcomings of centralised systems by utilising the advantages of permissioned blockchain technology to guarantee secure data sharing between IoT devices,

4-2975 | 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.2025.1203054

non-repudiation, and tamper-proof data storage. Throughout the data lifecycle—from initialisation and registration to data access control, validation, and sharing—it integrates a number of security measures, such as hashing, encryption, QR code-based encryption, and OTP-based passwords. This method offers a more dependable and durable solution for smart cities by strengthening the entire security posture of IoT applications and guaranteeing that private information is shielded from unwanted access and manipulation.

Proposed System Advantages

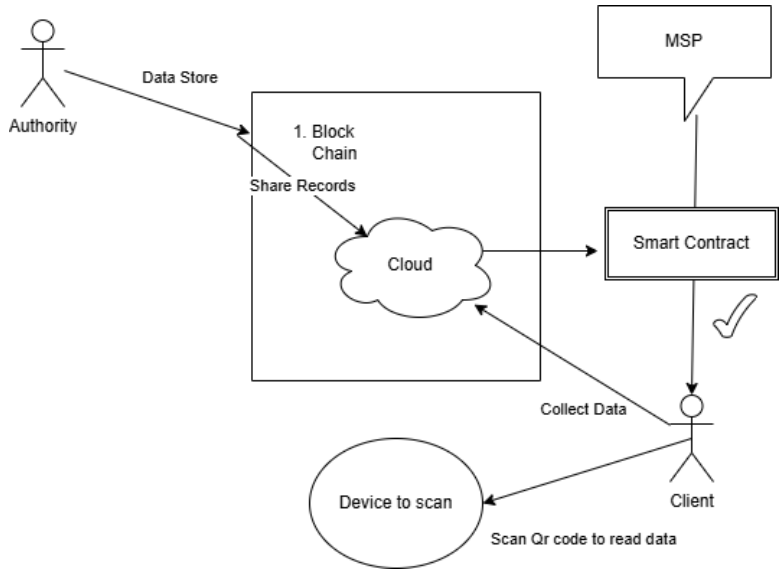
Efficient Cryptographic Techniques.

Enhanced Protection Against Cyber-attacks.

Multiple security phases, including data protection, authentication, access control, validation, and data sharing, to provide a holistic security solution for smart city IoT applications.

IV. SYSTEM ARCHITECTURE

The SecPrivPreserve framework's suggested system architecture is built around a permissioned blockchain network to guarantee the safe, private, and impenetrable management of Internet of Things data in smart cities. The Client, which gathers and submits data; the Authority, which controls data permissions and policies; the Membership Service Provider (MSP), which issues certificates and keeps a reliable network; and the Smart Contract (SC), which automates digital asset transfers and transaction verification, are some of the main parts of the architecture. Furthermore, transactions are validated by Endorsing Peers (EP), grouped into blocks by Ordering Peers (OP), and updated in the ledger by Committing Peers (CP). Peers in the same organisation can communicate securely thanks to channels. The decentralised architecture guards against unwanted changes and improves transparency while guaranteeing data integrity, non-repudiation, and fine-grained access control.



IV. METHODOLOGY

Creating a thorough plan to test the basic functionality and unique features across a range of platform combinations is the first step in the testing process. Strict methods of quality control are employed. The procedure confirms that the application is error-free and satisfies the specifications listed in the system requirements document. The following factors were taken into account when creating the framework based on the testing approaches.

MODULES:

1. Design of User Interfaces

To connect with server user must give their username and password then only they can able to connect the server. If the user already exits 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.

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

4-2975 | 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.2025.1203054

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 plays the main part of the project role. Authority login first then its with his registration data and store his data inside cloud.

4.Smart Contract
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 predetermine 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 register and then login into the application, the registration details are stored inside database. After User Login he will directly navigate User home page and Access data by searching with keyword. When data owner upload data the data will be encrypted the encrypted keys will be stored inside database and keys will shred with key repository.

V. IMPLEMENTATION

1. Advanced Encryption Standard, or AES The SecPrivPreserve framework uses the popular symmetric encryption technique AES (Advanced Encryption Standard) to secure IoT data in smart city applications. A 128-bit key length is used to encrypt sensitive data, guaranteeing confidentiality and security both during transmission and storage. Because of its speed, security, and compatibility with both hardware and software implementations, AES is recommended. Client information is encrypted in this system prior to being posted to the blockchain network. Secure key management is necessary because the same key is used for both encryption and decryption. For increased confidentiality, AES combines with other cryptographic methods such as Chebyshev polynomials.

2. Smart Contract The SecPrivPreserve system relies heavily on smart contracts to facilitate automated, impenetrable transactions across the blockchain network. These self-executing programs provide efficiency and confidence by carrying out predetermined agreements without the need for middlemen. Important tasks including data registration, transaction validation, QR code-based authentication, and safe key distribution are managed by smart contracts in this design. They automatically verify data uploads, regulate access, and enable safe downloads based on user credentials and access policies after being implemented on the permissioned blockchain. By safely logging each transaction on the immutable distributed ledger, smart contracts improve the system's dependability, transparency, and auditability.

VI. EXPERIMENTAL RESULT

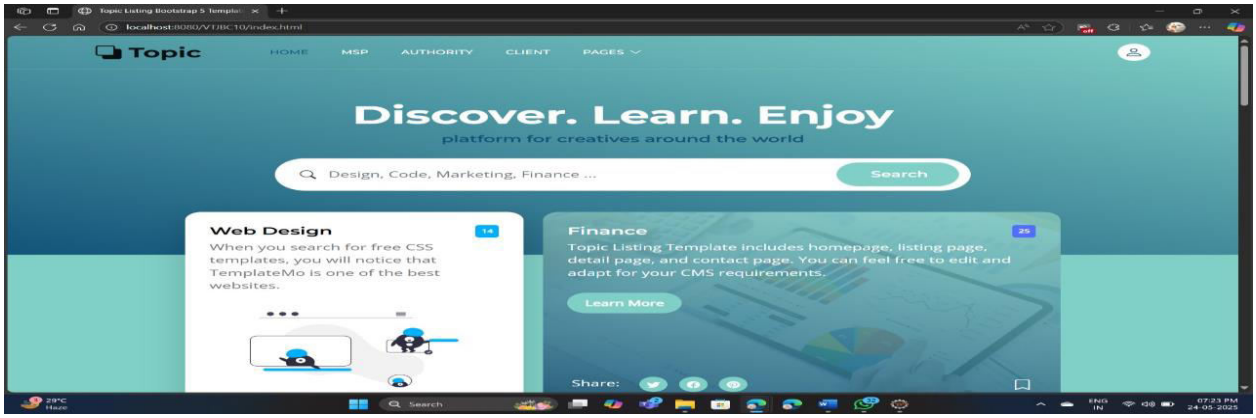


Fig 1. Home Page

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

4-2975 | 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.2025.1203054

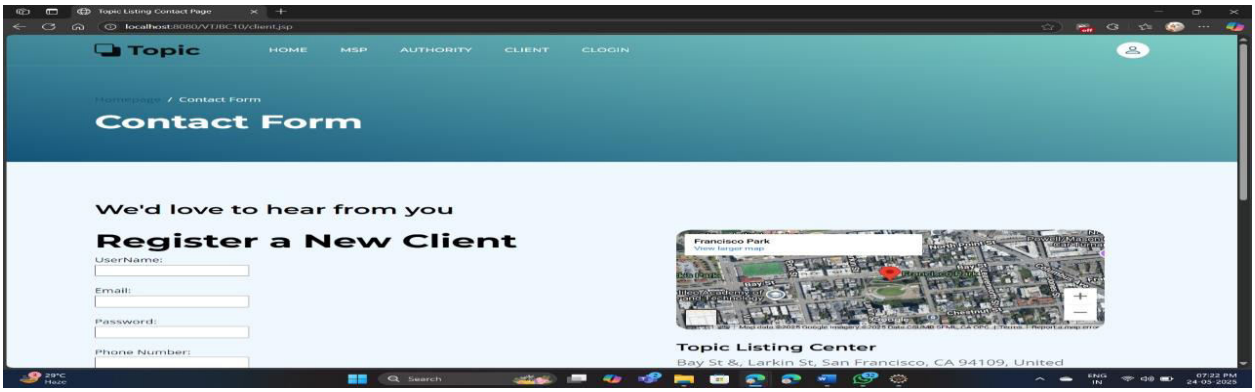


Fig 2. Client Registration Page

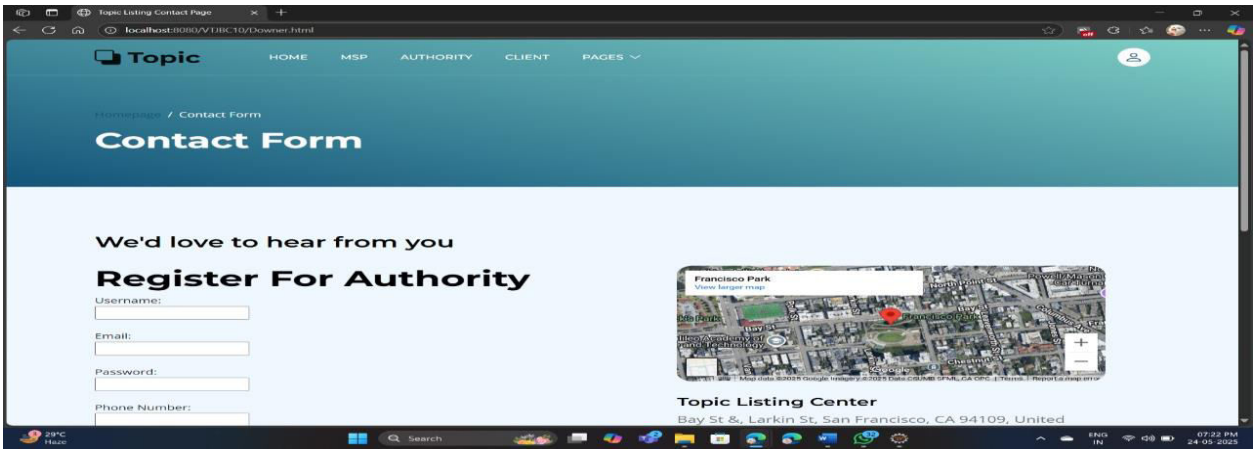


Fig 3. Authority Registration Page

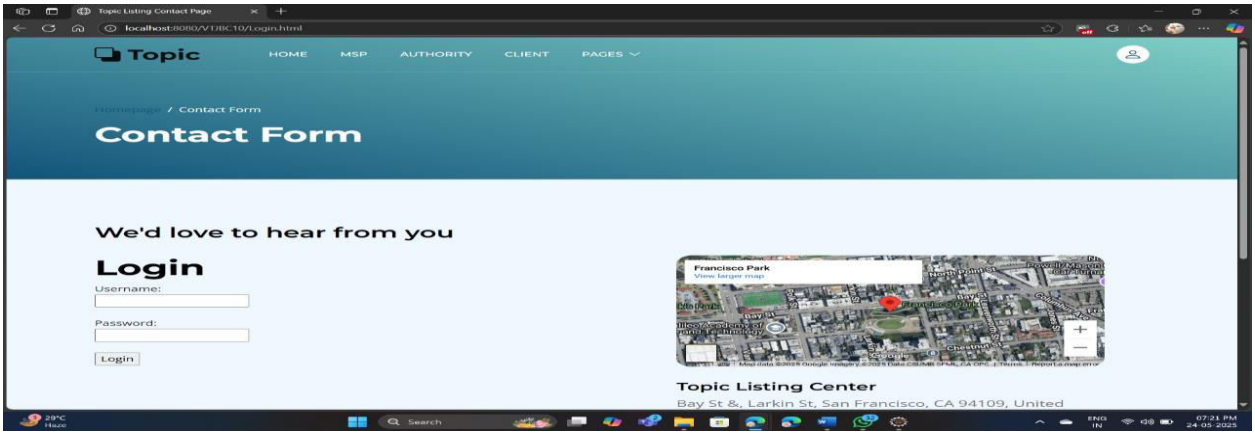


Fig 4. Login Page

VII.CONCLUSION

A complete, decentralised solution for improving the security, privacy, and integrity of IoT data in smart city applications is provided by the suggested SecPrivPreserve framework. Particularly in dynamic IoT situations, traditional centralised systems have shown themselves susceptible to data breaches, illegal access, and tampering. The system guarantees safe data sharing across heterogeneous devices, non-repudiation, and tamper-proof records by utilising permissioned blockchain technology. To protect sensitive data at every stage of its lifetime, from collection

4-2975 | 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.2025.1203054

and storage to access and sharing, it incorporates cutting-edge security features including AES encryption, hashing, and QR code-based authentication.

The system is more resilient to many types of cyberattacks thanks to its multi-phase security approach, which covers initialisation, registration, data protection, authentication, validation, and safe downloads. Furthermore, by automating access control and transaction validation, smart contracts remove middlemen and improve system transparency. The framework uses trustworthy cryptographic algorithms and the decentralised infrastructure of blockchain to address important challenges including data confidentiality, privacy dangers, and integrity threats.
In general, SecPrivPreserve effectively addresses the drawbacks of current solutions and illustrates how blockchain-integrated architectures may be used to secure IoT-enabled smart cities. By providing scalability, effective key management, and more robust privacy-preserving mechanisms appropriate for developing smart urban environments and vital data-centric services, the project lays the groundwork for future improvements.
.

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 Editors of Encyclopaedia. (Dec. 9, 2023). United Nations Population Fund. Encyclopedia 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 Web Conf. Web Conf., 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 IoTblockchain 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 Intell. Humanized 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.
[13] 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.
[14] 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.
[15] 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.
[16] 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.
[17] 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.
[18] 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.
[19] 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.

4-2975 | 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.2025.1203054

[20] 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.
[21] 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.
[22] 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.
[23] 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.
[24] 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.
[25] 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.
[26] I. Makhdoom, I. Zhou, M. Abolhasan, J. Lipman, and W. Ni, ''PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities,'' Comput. Secur., vol. 88, Jan. 2020, Art. no. 101653.
[27] 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.
[28] M. Šarac, N. Pavlović, N. Bacanin, F. Al-Turjman, and S. Adamović, ''Increasing privacy and security by integrating a blockchain secure interface into an IoT device security gateway architecture,'' Energy Rep.
[29] Q. Fan, J. Chen, L. J. Deborah, and M. Luo, ''A secure and efficient authentication and data sharing scheme for Internet of Things based on blockchain,'' J. Syst. Archit., vol. 117, Aug. 2021, Art. no. 102112.
[30] A. Manzoor, A. Braeken, S. S. Kanhere, M. Ylianttila, and M. Liyanage, ''Proxy re-encryption enabled secure and anonymous IoT data sharing platform based on blockchain,'' J. Netw. Comput. Appl., vol. 176, Feb. 2021, Art. no. 102917.
[31] M. Shen, X. Tang, L. Zhu, X. Du, and M. Guizani, ''Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities,'' IEEE Internet Things J., vol. 6, no. 5, pp. 7702–7712, Oct. 2019.
[32] J. Hong, ''Chaincomm: A framework for future communities based on blockchain,'' in Proc. IEEE 8th Int. Conf. Comput. Commun. (ICCC), Dec. 2022, pp. 1324–1328.
[33] A. Simonet-Boulogne, A. Solberg, A. Sinaeepourfard, D. Roman, F. Perales, G. Ledakis, I. Plakas, and S. Sengupta, ''Toward blockchainbased fog and edge computing for privacy-preserving smart cities,'' Frontiers Sustain. Cities, vol. 4, p. 136, Sep. 2022.
[34] D. L. Fekete and A. Kiss, ''A survey of ledger technology-based databases,'' Future Internet, vol. 13, no. 8, p. 197, 2021.
[35] 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,'' Proc. ACM Manage. Data, vol. 1, no. 2, pp. 1–27, 2023.
[36] X. Yang, Y. Zhang, S. Wang, B. Yu, F. Li, Y. Li, and W. Yan, ''LedgerDB: A centralized ledger database for universal audit and verification,'' Proc. VLDB Endowment, vol. 13, no. 12, pp. 3138–3151, Aug. 2020.

International Journal of Advanced Research in Education and Technology

ISSN: 2394-2975 Impact Factor: 8.152

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