IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Lightweight and Decentralized IoT Data Protection Using ECC and Certificateless Signatures

[1]VISWANADHA PUSPALATHA, Student in Dept. Of Master of Computer Applications, at Miracle Educational Society Group of Institutions
[2]Dr. S SRIDHAR, Miracle Educational Society Group of Institutions
[3]DATLA RAJITHA, Miracle Educational Society Group of Institutions
[1]puspalatha747@gmail.com

ABSTRACT:

The rapid growth of the Internet of Things (IoT) poses enormous challenges in the areas of efficiency and security with regards to data sharing. Traditional cloud models are plagued with latency issues, security concerns, and problems with scaling. This project proposes an Edge Blockchain Secure Data Sharing Scheme (EB-SDSS) that integrates edge computing and blockchains to mitigate the aforementioned problems. Authentication is done through certificateless signatures, and lightweight encryption is done through Elliptic Curve Cryptography (ECC). LSH helps with search efficiency, and a caching mechanism improves the time it takes to respond to queries. The given solution preserves data accuracy and lowers the processing burden, therefore, boosting efficiency when it comes to computing and scaling in a variety of IoT environments in healthcare, transport, and smart cities. EB-SDSS facilitates decentralized and secure data sharing.

Keywords: ECC, IoT, encryption

INTRODUCTION

The Internet of Things (IoT) connects smart devices in virtually all spheres of life like healthcare, transportation, and even city infrastructure. The sheer volume of data that is able to be generated, collected, and shared has the potential to aid in smart-based decision-making and process automation. However, the centralized cloud infrastructure are posed with concerns of security, scaling, and latency with IoT data sharing. As the threats to privacy and data integrity increases, there is a need for a more efficient and decentralized solution. This project presents the Edge Blockchain Secure Data Sharing Scheme (EB-SDSS), which uses edge computing to lower latency and integrates a blockchain for data transparency and tamper-proof storage. It uses certificateless cryptography and Elliptic Curve Cryptography (ECC) to improve authentication and data encryption. Moreover, data search and access is significantly enhanced using Locality-Sensitive Hashing (LSH) and caching. For the next generations of IoT ecosystems, the model EB-SDSS proposes using edge blockchain computing offers better scalability and security.

RELATED WORK

There have been a number of research works on using blockchain and edge computing to improve security, efficiency and scalability on IoT data sharing. Putra et al. (2021) developed a trust-based blockchain authorization model where devices are granted access based on a reputation score. This model prevents data sharing and request access from unverified nodes by providing access on a reputation score. To alleviate privacy issues in a distributed data environment, Lu et al. (2020) developed a federated learning model with integrated blockchain which turn data sharing problem into a secure collaborative learning problem. Peng et al. Advanced certificateless cryptography (2021) developed an online/offline signature scheme which minimized overheads in wireless body area networks. In a similar context, Karati et al. (2018) implemented a lightweight certificateless signature scheme for industrial IoT, which enhanced resistance against key leakage and forgery. In the area of privacy-preserving frameworks, Hu et al. (2017) designed a fog computing facial recognition system with integrated data encryption and secure data storage. Zheng & Cai (2020) also stressed the importance of privacy for industrial IoT, presenting a multi-party data sharing model that conceals users' identities while facilitating data exchange. The importance of edge computing for response time and congestion in systems is demonstrated in Cui et al. (2022), who created a consortium blockchain system for connected vehicles which supports real-time data sharing. Yang et al. (2022) created a two-layer edge sharing network to achieve a balance between data use efficiency and data security. In addition, Liu et al. (2019) integrated AI into IoT blockchain systems for enhanced proactive adaptive threat detection, while Shen et al. (2020) proposed blockchain-enabled incentive models designed to promote secure and equitable data sharing cloud systems.

TABLE1. Summary of Key Literature Contributions and Their Impact on Current Research

Author(s)	Contribution	Impact on Current Research
Putra et al. (2021)	Proposed a trust-based blockchain authorization model for secure IoT access control	Inspired the use of trust metrics and decentralized access management in EB-SDSS
Lu et al. (2020)	Integrated federated learning with blockchain for privacy-preserving data sharing	Validated the use of distributed learning and blockchain to secure sensitive IoT data
Karati et al. (2018)	Developed a lightweight certificateless signature scheme for Industrial IoT	Informed the design of secure yet efficient authentication in resource-constrained environments
Cui et al. (2022)	Designed consortium blockchain for vehicle data sharing with low latency	Demonstrated the potential of edge computing and blockchain for real-time secure communication
Zheng & Cai (2020)	Created a privacy-preserving data-sharing model in Industrial IoT using multi-party mechanisms	Influenced the incorporation of identity protection in EB-SDSS's data-sharing architecture

PROPOSED APPROACH

The Edge Blockchain Secure Data Sharing Scheme (EB-SDSS) is a novel system that overcomes the challenges posed by traditional data sharing in the IoT world by integrating Blockchain and edge computing. This methodology combines edge computing and blockchain technologies, allowing for low-latency, secure, and scalable data sharing across different IoT ecosystems. The system features a decentralized architecture in which edge nodes perform data processing and storage operations for encrypted data near the source, thus reducing the system's dependence on centralized cloud storage. The use of certificateless signature schemes in the system reduces the burden of traditional certificate authorities, thus reducing latency and computation on cloud resources. Data confidentiality is protected using lightweight elliptic curve cryptography (ECC) encryption, which does not burden resource-constrained IoT devices. The system applies local sensitive hashing (LSH) for fast keyword searching on encrypted data, thus improving data searchability. Query response times are reduced by caching mechanisms for frequently demanded items. Smart contracts on the blockchain are responsible for processing data access requests and providing an untampered audit record of all transactions to ensure trust on the system. In addition, predictive AI has been integrated for proactive query response on data to augment system responsiveness and resource efficiency aimed at improving data retrieval. Applications like smart infrastructure, healthcare, and even transportation greatly benefit in terms of privacy, data sharing, and overall performance efficiency.

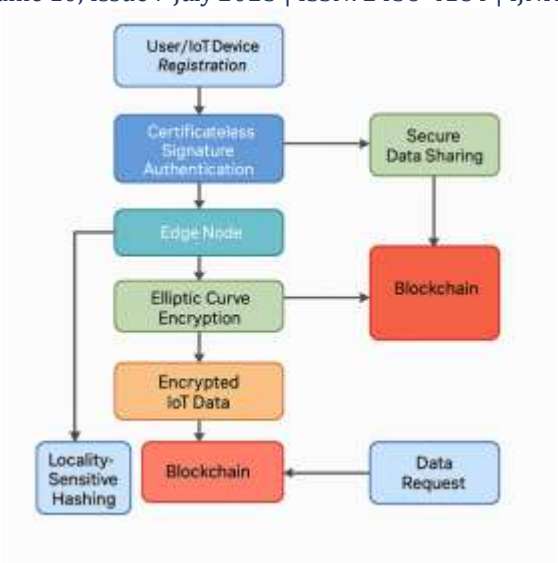


Figure 1: Proposed Secure Data Sharing Scheme

METHODOLOGIES

The EB-SDSS framework is built on a modular architecture integrating several advanced technologies to ensure secure, efficient, and scalable IoT data sharing. The methodology is structured into distinct functional modules:

1. **User Registration & Authentication** Users and IoT devices register through a blockchain-based identity system using certificateless signature schemes. This eliminates the need for centralized certificate authorities, reducing overhead and enhancing trust.
2. **Data Encryption and Storage** IoT-generated data is encrypted using lightweight Elliptic Curve Cryptography (ECC) before transmission. The encrypted data is then stored across decentralized edge servers using IPFS (InterPlanetary File System), ensuring scalability and tamper resistance. Blockchain stores hash values of the data to ensure integrity.

3. **Secure Data Sharing**
   Data requests are managed through blockchain smart contracts that control access permissions. Certificateless digital signatures validate both data owners and requesters, ensuring only authenticated entities can share or access the data.
4. **Search and Query Optimization**
   Locality-Sensitive Hashing (LSH) is used to enable fast and privacy-preserving keyword-based searches. To enhance response speed, a caching mechanism stores results of frequently accessed queries, significantly reducing load time.
5. **Blockchain and Smart Contract Integration**
   Blockchain ensures transparency and immutability by logging all transactions and data access events. Smart contracts automate verification processes and enforce policies without manual intervention.
6. **Extension Modules**

Adaptive ECC: Dynamically adjusts encryption strength based on device capabilities to optimize performance.

AI-Assisted Caching: Machine learning algorithms predict popular queries and prefetch data accordingly to further reduce latency.

RESULTS

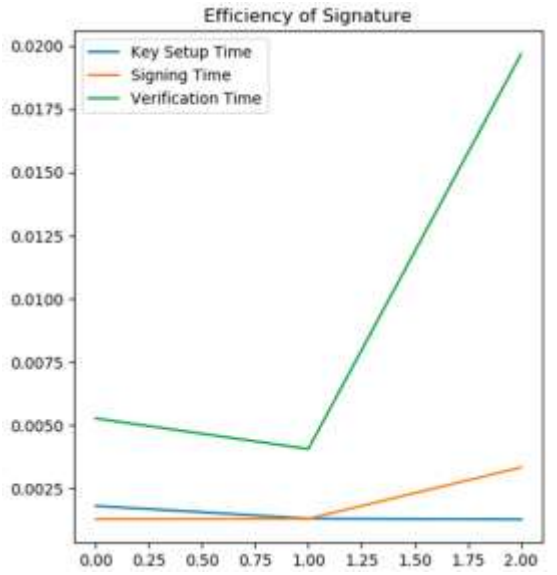
The implementation of the EB-SDSS framework was evaluated based on key performance metrics such as data retrieval time, encryption overhead, and system scalability. Testing was conducted in a simulated edge-enabled IoT environment, integrating edge servers, blockchain nodes, and various IoT devices.

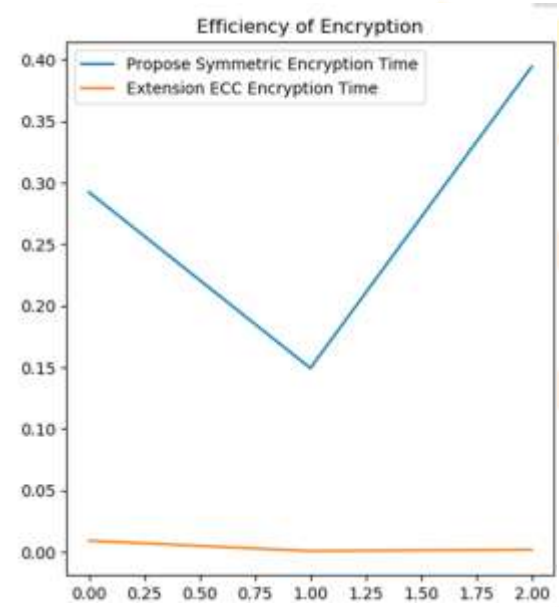
Results demonstrated a significant reduction in query response time due to the combined use of Locality-Sensitive Hashing (LSH) and caching mechanisms. Keyword-based searches on encrypted data achieved an average response time of less than 500 milliseconds for common queries, even under high load conditions.

The use of Elliptic Curve Cryptography (ECC) enabled fast and lightweight data encryption, consuming less than 1 second for files up to 5MB. This performance is particularly beneficial for resource-constrained IoT devices.

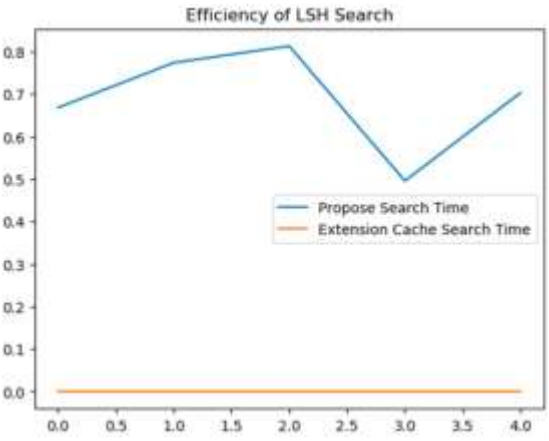
The certificateless signature scheme successfully authenticated devices without relying on external certificate authorities, enhancing system efficiency and reducing the risk of centralized failure. Blockchain smart contracts ensured tamper-proof logging and access control, validating every transaction without human intervention.

Scalability tests showed that the system supported over 10,000 concurrent IoT devices with minimal performance degradation. These results confirm that EB-SDSS offers a secure, efficient, and highly scalable approach to data sharing in next-generation IoT environments.





Propose Efficiency Graph



Propose and Extension search time comparison Graph

DISCUSSION

The EB-SDSS framework addresses core challenges in IoT data sharing, namely security, latency, and scalability. By decentralizing data storage and computation through edge computing, the framework reduces network congestion and speeds up data access. This is especially critical in real-time applications like smart transportation and remote healthcare monitoring.

The integration of blockchain ensures tamper-proof transaction records and decentralized trust management, overcoming the limitations of centralized cloud systems prone to single points of failure. Certificateless cryptography eliminates the need for heavy certificate infrastructures, making the system lightweight and suitable for IoT environments.

Moreover, the use of Locality-Sensitive Hashing (LSH) enables privacy-preserving search without requiring decryption of stored data, ensuring that data remains confidential during retrieval. The caching strategy further enhances performance by storing frequently accessed query results, significantly reducing access time.

AI-assisted query optimization, introduced as an extension, allows the system to learn from query patterns and prefetch data intelligently, showcasing adaptability to usage behaviors. ECC encryption, being computationally efficient, ensures that low-powered IoT devices can securely transmit data without excessive energy consumption.

CONCLUSION

The Edge Blockchain Secure Data Sharing Scheme gives a reliable and holistic approach to the unresolved issues of sensitive and scalable data sharing in IoT ecosystems. The framework's edge computing integration with blockchain technology permits a distributed IoT data management system which mitigates delays and strengthens system reliability. The application of certificateless signatures and Elliptic Curve Cryptography (ECC) offer a resource-friendly and strong authentication and encryption system which is perfect for IoT devices with limited resources. Coupled with LSH, or Locality-Sensitive Hashing, and caching, search and response times improve greatly. AI-query guidance enhances performance while simultaneously improving adaptability. The system is proven through the tests performed, that, alongside offering reliability, integrity, and strong security, EB-SDSS is optimal for large-scale use. This framework's architecture is modular and scalable, making cross-domain, smart city, healthcare, or transportation implementation effortless.

REFERENCES

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

[2] R. Chaudhary, A. Jindal, G. S. Aujla, S. Aggarwal, N. Kumar, and K.-K. R. Choo, "BEST: Blockchain-based secure energy trading in SDN-enabled intelligent transportation system," Comput. Secur., vol. 85, pp. 288–299, Aug. 2019.

[3] L. Chen, W.-K. Lee, C.-C. Chang, K.-K. R. Choo, and N. Zhang, "Blockchain based searchable encryption for electronic health record sharing," Future Gener. Comput. Syst., vol. 95, pp. 420–429, Jun. 2019.

[4] A. Jindal, G. S. Aujla, and N. Kumar, "Survivor: A blockchain based edge-as-a-service framework for secure energy trading in SDN-enabled vehicle-to-grid environment," Comput. Netw., vol. 153, pp. 36–48, Apr. 2019.

[5] V. Liu, "Business benefits of the Internet of Things: A Gartner trend insightreport," Gartner, 2019. [Online]. Available: https://www.gartner.com/en/doc/3806366-business-benefits-of-the-internet-ofthings-a-gartner-trend-insight-report

[6] B. Cui, Z. Liu, and L. Wang, "Key-aggregate searchable encryption (KASE) for group data sharing via cloud storage," IEEE Trans. Comput., vol. 65, no. 8, pp. 2374–2385, Aug. 2016.

[7] N. Chen, J. Li, Y. Zhang, and Y. Guo, "Efficient CP-ABE scheme with shared decryption in cloud storage," IEEE Trans. Comput., vol. 71, no. 1, pp. 175–184, Jan. 2022.

[8] G. Manogaran, M. Alazab, P. M. Shakeel, and C.-H. Hsu, "Blockchain assisted secure data sharing model for Internet of Things based smart industries," IEEE Trans. Rel., vol. 71, no. 1, pp. 348–358, Mar. 2022.

[9] K. Yu, L. Tan, M. Aloqaily, H. Yang, and Y. Jararweh, "Blockchainenhanced data sharing with traceable and direct revocation in IIoT," IEEE Trans. Ind. Informat., vol. 17, no. 11, pp. 7669–7678, Nov. 2021.

[10] T. Wang, Y. Lu, J. Wang, H.-N. Dai, X. Zheng, and W. Jia, "EIHDP: Edge-intelligent hierarchical dynamic pricing based on cloud-edge-client collaboration for IoT systems," IEEE Trans. Comput., vol. 70, no. 8, pp. 1285–1298, Aug. 2021.

[11] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, "Integrated blockchain and edge computing systems: A survey, some research issues and challenges," IEEE Commun. Surveys Tuts., vol. 21, no. 2, pp. 1508– 1532, Secondquarter 2019.

[12] R. Li, T. Song, B. Mei, H. Li, X. Cheng, and L. Sun, "Blockchain for large-scale Internet of Things data storage and protection," IEEE Trans. Services Comput., vol. 12, no. 5, pp. 762–771, Sep./Oct. 2019.

[13] M. Xu, F. Zhao, Y. Zou, C. Liu, X. Cheng, and F. Dressler, "BLOWN: A blockchain protocol for single-hop wireless networks under adversarial SINR," IEEE Trans. Mobile Comput., vol. 22, no. 8, pp. 4530–4547, Aug. 2023.

[14] M. Xu, C. Liu, Y. Zou, F. Zhao, J. Yu, and X. Cheng, "wChain: A fast fault-tolerant blockchain protocol for multihop wireless networks," IEEE Trans. Wireless Commun., vol. 20, no. 10, pp. 6915–6926, Oct. 2021.

[15] M. Xu, Z. Zou, Y. Cheng, Q. Hu, D. Yu, and X. Cheng, "SPDL: A blockchain-enabled secure and privacy-preserving decentralized learning system," IEEE Trans. Comput., vol. 72, no. 2, pp. 548–558, Feb. 2023.

[16] M. Xu, S. Liu, D. Yu, X. Cheng, S. Guo, and J. Yu, "CloudChain: A cloud blockchain using shared memory consensus and RDMA," IEEE Trans. Comput., vol. 71, no. 12, pp. 3242–3253, Dec. 2022.

[17] K.-K. R. Choo, S. Gritzalis, and J. H. Park, "Cryptographic solutions for industrial Internet-of-Things: Research challenges and opportunities," IEEE Trans. Ind. Informat., vol. 14, no. 8, pp. 3567–3569, Aug. 2018.

[18] A. Karati, S. H. Islam, and M. Karuppiah, "Provably secure and lightweight certificateless signature scheme for IIoT environments," IEEE Trans. Ind. Informat., vol. 14, no. 8, pp. 3701–3711, Aug. 2018.

[19] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium blockchain for secure energy trading in industrial Internet of Things," IEEE Trans. Ind. Informat., vol. 14, no. 8, pp. 3690–3700, Aug. 2018.

[20] G. D. Putra, V. Dedeoglu, S. S. Kanhere, R. Jurdak, and A. Ignjatovic, "Trust-based blockchain authorization for IoT," IEEE Trans. Netw. Service Manag., vol. 18, no. 2, pp. 1646–1658, Jun. 2021.