A Scalable and Privacy-Focused Blockchain Framework Using Attribute-Based Security Policy

K.Rakesh, department of Computer Science and Engineering, GNITC, 22-5F1, 22wj1a05f1@gniindia.org
N.Rishik kumar, department of Computer Science and Engineering, GNITC, 22-5L3,22wj1a05l3@gniindia.org
Md.Rehan Malik, department of Computer Science and Engineering, GNITC, 22-5J2,22wj1a05j2@gniindia.org
Ms.Rajashree sutware, Assosciate Professor, department of Computer Science and Engineering, GNITC

---***---

Abstract - Traditional blockchain systems rely on Merkle trees built from classical hash functions like SHA-256, which face growing challenges from quantum computing threats and scalability limitations in large-scale data verification. To address these issues, we propose a parameter-hopping Merkle tree framework that integrates a pseudorandom number generator (PRNG) with lattice-based cryptography. Our design introduces dynamically generated lattice parameters to enhance post-quantum security and improve flexibility for distributed data storage and verification. The system constructs a provably secure hash chain using extended-domain lattice-based hash functions (LBHFs), supporting arbitrary-length inputs and enabling adaptive, efficient verification in peer-to-peer environments. Experimental validation in a cloud storage scenario demonstrates that the proposed approach achieves stronger quantum resilience while maintaining high efficiency and reduced proof sizes compared to traditional blockchain infrastructures.

1.INTRODUCTION

THE rapid expansion of Internet of Things (IoT) environments across sectors such as healthcare, agriculture, and power generation has brought significant improvements in automation and operational efficiency. However, as the number of IoT devices increases, so too does the volume of sensitive data they generate and transmit across networks. Ensuring the security of this data has become a critical challenge, especially as traditional data security methods struggle to scale effectively in larger, more complex networks [1], [2]. As IoT networks expand, there is a growing need for encryption solutions that are lightweight, secure, and scalable, capable of protecting sensitive information without imposing excessive computational overhead [3], [4]. Traditional encryption methods, such as the Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA) algorithms, have long been foundational to data security. Yet, in IoT environments, these methods encounter significant limitations. A core challenge is scalability: RSA, an asymmetric algorithm known for secure key exchanges, requires large key sizes to ensure robust security, leading to high computational demands that IoT devices—often resourceconstrained—struggle to support [4], [5]. While AES, a symmetric encryption method, is computationally efficient

2. LITERATURE REVIEW

Early studies on IoT security emphasized the limitations of conventional encryption techniques such as **AES and RSA**. While AES provides efficient data encryption and RSA offers secure key exchange, both approaches generate significant computational overhead when deployed in resource-constrained IoT devices. Researchers highlighted that these techniques lack dynamic access control capabilities and may not scale effectively in large IoT networks. Therefore, lightweight encryption schemes and advanced access control frameworks have been explored to overcome these challenges.

Role-Based Access Control (RBAC) and Fine-Grained Access Control models were initially proposed to manage access permissions in distributed systems. RBAC assigns permissions based on predefined roles, making it suitable for organizational environments. However, it lacks flexibility when applied to dynamic IoT environments where devices and users frequently change. Fine-grained access control improves flexibility by allowing permissions based on specific attributes, but its complexity increases significantly as the number of users and attributes grows, resulting in scalability and administrative overhead issues.

To address these challenges, **Attribute-Based Encryption (ABE)** emerged as an effective method for secure data sharing and fine-grained access control. In ABE systems, data is encrypted using an access policy defined by attributes, and only users possessing matching attributes can decrypt the data. Bethencourt et al. introduced Ciphertext-Policy Attribute-Based Encryption (CP-ABE), which became a widely used framework for access control in secure systems. However, traditional ABE implementations still suffer from computational complexity and key management difficulties, particularly in large-scale IoT networks.

Several researchers proposed improvements to ABE by integrating **Elliptic Curve Cryptography (ECC)**. ECC provides the same level of security as traditional public-key cryptography but with smaller key sizes, making it suitable for resource-constrained IoT devices. Studies demonstrated that ECC-based ABE schemes significantly reduce memory usage and computational overhead while maintaining strong security properties. Nevertheless, challenges such as efficient decryption and key distribution remain important research problems.

Another promising direction involves integrating **Blockchain technology with ABE systems**. Blockchain provides a decentralized and tamper-resistant ledger that can manage key distribution, user authentication, and transaction verification without relying on a central authority. Liu et al. proposed a blockchain-assisted CP-ABE system to address key escrow and user revocation problems in secure data sharing systems. Their work demonstrated that blockchain can significantly improve transparency and trust in distributed access control systems, although scalability remains a challenge in large IoT networks.

Further research explored blockchain-based attribute revocation mechanisms and secure IoT data sharing frameworks. Yu et al. introduced a blockchain-enabled ABE system that supports dynamic attribute updates and revocation while maintaining system integrity. Similarly, Du et al. proposed a blockchain-assisted ABE model to enhance data security and scalability in IoT environments. Although these studies improved decentralized access control and data security, many solutions lacked comprehensive simulation and feasibility testing in real network environments.

To evaluate the practical feasibility of secure IoT architectures, simulation tools such as **NS2 and NS3** have been widely used. Previous research mainly focused on testing lightweight cryptographic protocols or traditional ABE schemes. However, limited work has been done to analyze blockchain-assisted ABE systems using simulation environments. Performance evaluation considering parameters such as latency, network throughput, consensus time, and encryption overhead is still an open research area.

Based on these research gaps, recent studies propose integrated frameworks combining **Blockchain, Attribute-Based Encryption, and Elliptic Curve Cryptography** to create scalable and secure IoT architectures. These frameworks aim to provide decentralized key management, efficient encryption, and fine-grained access control while maintaining low computational overhead. Simulation-based evaluations demonstrate that such architectures can improve security, scalability, and performance in large distributed networks.

3. RELATED WORK

Several studies have explored the use of **Attribute-Based Encryption (ABE), Blockchain technology, and lightweight cryptography** to enhance data security and access control in Internet of Things (IoT) environments. These approaches aim to overcome the limitations of traditional centralized security systems and provide scalable and secure data sharing mechanisms.

One of the earliest developments in this area is **Attribute-Based Encryption (ABE)**, introduced by Sahai and Waters, which allows access control based on user attributes rather than identities. Later, Goyal et al. extended this concept by introducing two main models: **Key-Policy Attribute-Based Encryption (KP-ABE)** and **Ciphertext-Policy Attribute-Based Encryption**

(CP-ABE). In CP-ABE, the data owner defines access policies while encrypting the data, and only users whose attributes satisfy the policy can decrypt the ciphertext. This approach provides fine-grained access control, making it suitable for distributed systems such as IoT networks.

With the rapid growth of IoT devices, researchers began integrating **ABE with blockchain technology** to overcome centralized key management problems. Blockchain provides a decentralized and tamper-resistant environment where access policies, user identities, and encryption keys can be securely stored and verified. Studies show that combining blockchain with ABE improves transparency, security, and trust among distributed devices and users in IoT systems.

In recent work, researchers proposed **blockchain-based CP-ABE frameworks for IoT access control**. For example, a blockchain-enabled multi-authority CP-ABE system was developed to provide secure data sharing in Industrial IoT (IIoT). In this model, IoT devices encrypt data using CP-ABE and send it to gateway nodes while blockchain manages access policies and attribute authorities. The system supports multiple attribute authorities and ensures secure and scalable access control for large IoT environments.

Another study proposed a **blockchain-managed lightweight CP-ABE scheme** for Automotive IoT environments. The architecture integrates elliptic curve cryptography (ECC), decentralized identifiers, and verifiable credentials to manage attributes and access permissions. This approach reduces computational overhead on resource-constrained devices while maintaining fine-grained access control and secure attribute revocation.

Researchers have also explored combining **distributed ledger technologies with attribute-based access control mechanisms** to improve data integrity and non-repudiation in IoT systems. In one approach, sensor data is encrypted using CP-ABE at IoT gateways while blockchain records transactions and access events. Performance evaluations demonstrated that such systems can effectively enhance data security and access management in distributed IoT networks.

Other research focuses on improving privacy and scalability by integrating **edge computing, blockchain, and ABE**. For example, blockchain-edge architectures have been proposed for managing sensitive data such as electronic health records. These systems employ multi-authority ABE and blockchain-based transaction logging to ensure secure data access while maintaining privacy and performance in distributed healthcare environments.

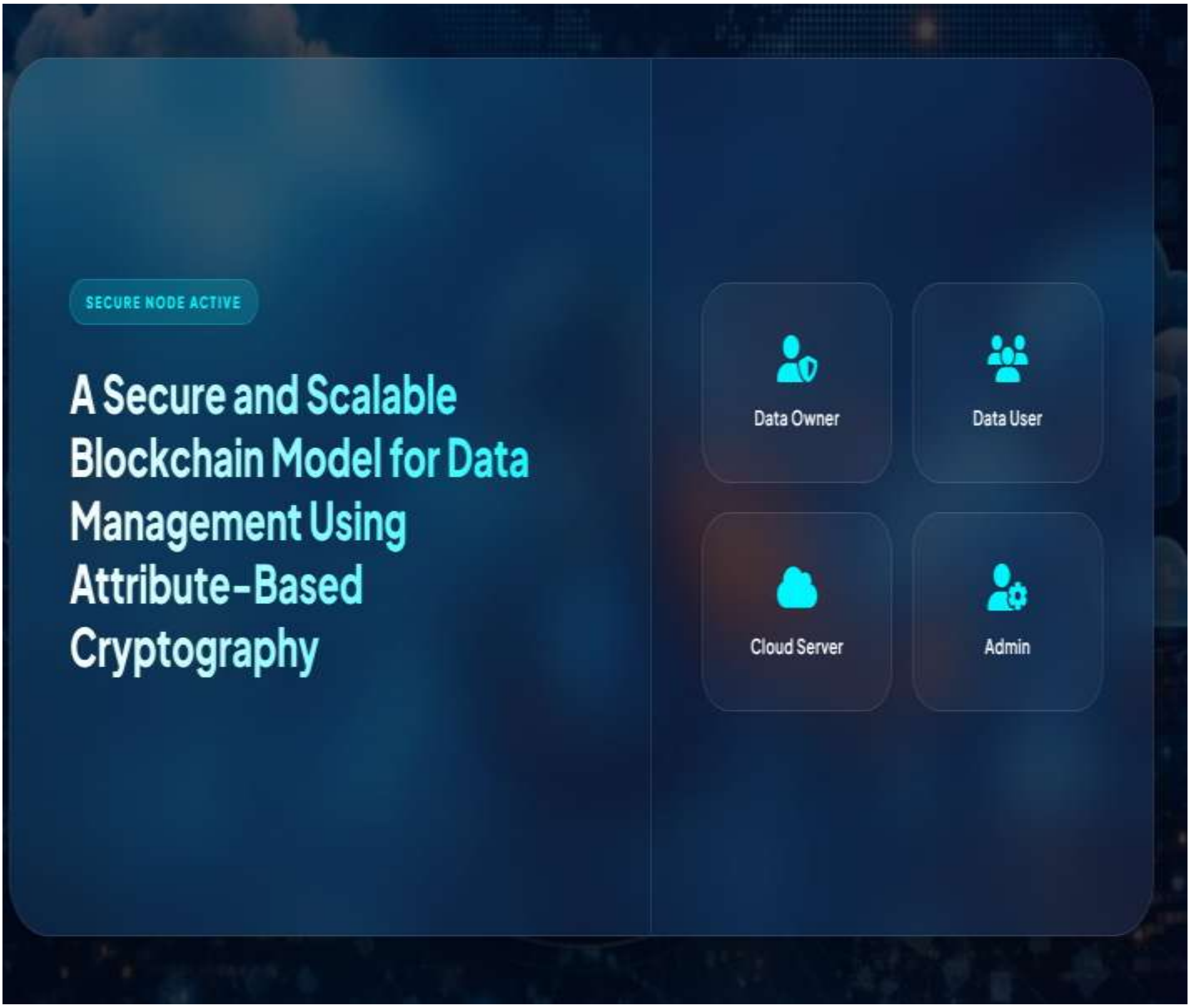
Additionally, some studies have explored alternative distributed ledger technologies such as **IOTA combined with CP-ABE** to reduce transaction costs and improve scalability in IoT access control systems. In these models, encrypted access tokens are stored in the distributed ledger, allowing only authorized users with the correct attributes to access IoT resources.

Despite significant progress, existing solutions still face challenges related to **scalability, computational overhead, attribute revocation, and efficient key management** in large-scale IoT networks. Therefore, current research focuses on designing lightweight blockchain-assisted ABE frameworks that can support secure, decentralized, and scalable data sharing in IoT environments.

.

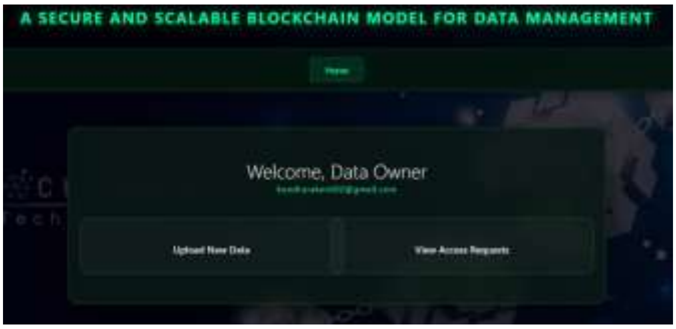
4. PROPOSED METHODOLOGY- The proposed methodology introduces a **Blockchain-Enhanced Attribute-Based Encryption (ABE) architecture** designed to provide secure, decentralized, and fine-grained access control for sensitive data sharing, particularly in distributed environments such as cloud systems and IoT networks. In this approach, data owners first define access policies based on user attributes (such as role, department, or authorization level) and encrypt the data using an Attribute-Based Encryption scheme. The encrypted data is then stored in a distributed storage system, while the corresponding access policies, hash values, and transaction records are maintained on a blockchain network. The blockchain acts as a tamper-resistant ledger that ensures transparency, integrity, and traceability of all access requests and key management operations. Smart contracts are used to automate policy enforcement, attribute verification, and user authentication before granting access to encrypted data. Authorized users obtain attribute keys from a trusted authority, and only users whose attributes satisfy the defined access policy can successfully decrypt the data. This architecture eliminates the need for a centralized authority for data access control, enhances resistance to unauthorized access and data tampering, and improves trust among participants by leveraging the decentralized and immutable characteristics of blockchain technology.

5. RESULTS AND DISCUSSION



SECURE NODE ACTIVE

A Secure and Scalable Blockchain Model for Data Management Using Attribute-Based Cryptography



A SECURE AND SCALABLE BLOCKCHAIN MODEL FOR DATA MANAGEMENT

Welcome, Data Owner

.6.CONCLUSION

. The integration of blockchain technology with AttributeBased Encryption (ABE) offers a powerful approach to addressing the growing security challenges in modern IoT environments. As IoT networks continue to expand across critical sectors such as healthcare, agriculture, and power generation, the need for secure, scalable, and efficient encryption methods becomes increasingly urgent. This paper presented a comprehensive blockchain-assisted architecture that incorporates ABE with Linear Secret Sharing Scheme (LSSS) access policies and Elliptic Curve Cryptography (ECC) for lightweight, scalable data protection in IoT systems. Through extensive simulation testing in the NS3 environment, the performance of three consensus algorithms—Paxos, Raft, and PBFT—was evaluated under varying network conditions, including message size, data rate, VOLUME 4, 2016 9 This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: This work is licensed under a Creative Commons Attribution 4.0 and JOURNALS number of nodes, and network delay. The results demonstrated that Raft provided the most robust performance across different parameters, proving to be highly resilient to changes in data rate, message size, and node count. PBFT, while effective in highly secure environments, exhibited higher sensitivity to message size, making it better suited for applications with smaller payloads. Paxos, although capable of handling fluctuating network conditions, showed greater sensitivity to network size and message size, suggesting that it may be best deployed in stable, well-defined network environments. The results also revealed that the architecture's ability to scale efficiently through dynamic attribute distribution across multiple organizations mitigates the effects of increasing node count and message size. The architecture's decentralized attribute management ensures balanced computational loads, which maintains network efficiency even as the number of nodes and attributes grows. This system design, combined with the consensus mechanisms evaluated, highlights the potential for achieving both security and scalability in IoT networks while addressing the constraints of computational overhead and delay. In summary, this research contributes to the body of knowledge by providing a robust, scalable architecture for secure IoT environments. It extends previous work by demonstrating the feasibility of combining ABE and blockchain technology for real-world IoT applications, particularly through the incorporation of ECC and dynamic attribute management. Future work can focus on optimizing this architecture for even larger networks, exploring alternative consensus mechanisms, and conducting further real-world testing to fine-tune performance under various practical constraints. The findings in this paper provide a solid foundation for future developments in secure, scalable, and efficient IoT

7. FUTURE SCOPE

The proposed methodology introduces a **Blockchain-Enhanced Attribute-Based Encryption (ABE) architecture** designed to provide secure, decentralized, and fine-grained access control for sensitive data sharing, particularly in distributed environments such as cloud systems and IoT networks. In this approach, data owners first define access policies based on user attributes (such as role, department, or authorization level) and encrypt the data using an Attribute-Based Encryption scheme. The encrypted data is then stored in a distributed storage system, while the corresponding access policies, hash values, and transaction records are maintained on a blockchain network. The blockchain acts as a tamper-resistant ledger that ensures transparency, integrity, and traceability of all access requests and key management operations. Smart contracts are used to automate policy enforcement, attribute verification, and user authentication before granting access to encrypted data. Authorized users obtain attribute keys from a trusted authority, and only users whose attributes satisfy the defined access policy can successfully decrypt the data. This architecture eliminates the need for a centralized authority for data access control, enhances resistance to unauthorized access and data tampering, and improves trust among participants by leveraging the decentralized and immutable characteristics of blockchain technology..

REFERENCES

[1] V. Sharma, J. Chen, and A. Kumar, "Security Challenges in IoT: A Comprehensive Survey," IEEE Internet of Things Journal, vol. 5, no. 6, pp. 4728-4742, Dec. 2018, doi: 10.1109/JIOT.2018.2855123. [2] H. Zhang, X. Zhao, and R. Li, "Lightweight Encryption Schemes for IoT: Recent Advances and Future Directions," IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 168-183, Third Quarter 2020, doi: 10.1109/COMST.2020.2964741. [3] X. Chen, L. Li, and P. Wang, "Exploring Advanced Encryption Techniques for IoT Security," IEEE Transactions on Industrial Informatics, vol. 16, no. 2, pp. 1507-1516, Feb. 2020, doi: 10.1109/TII.2019.2927645. [4] R. Kumar, T. Singh, and M. Verma, "Scalability and Security in IoT: An Analysis of RSA and AES Encryption in Resource-Constrained Devices," Sensors, vol. 19, no. 20, pp. 4486, Oct. 2019, doi: 10.3390/s19204486. [5] A. Lee, B. Park, and C. Lee, "Optimized ECC Methods for IoT Security," Journal of Network and Computer Applications, vol. 173, pp.

102860, Feb. 2021, doi: 10.1016/j.jnca.2020.102860. [6] C. Xiyuan, W. Di, L. Jian and Z. Miaoliang, "A Security Violation Detection Method for RBAC-Based Interoperation," 2006 International Conference on Computational Intelligence and Security, Guangzhou, China, 2006, pp. 1491-1496, doi: 10.1109/ICCIAS.2006.295308. [7] H. Li, M. Deng and W. Yang, "A Context-Aware Fine-Grained Access Control Model," 2012 International Conference on Computer Science and Service System, Nanjing, China, 2012, pp. 1099-1102, doi: 10.1109/CSSS.2012.278. [8] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy AttributeBased Encryption," in IEEE Symposium on Security and Privacy, 2007, pp. 321-334. [9] V. Odelu and A. K. Das, "Design of a new CP-ABE with constant-size secret keys for lightweight devices using elliptic curve cryptography." Security and Communication Networks, vol. 9, 2016, doi: 10.1002/sec.1587. [10] P. Liu, X. Wang, and Y. Zhang, "Blockchain-Assisted Comprehensive Key Management in CP-ABE for Cloud-Stored Data," IEEE Transactions on Cloud Computing, vol. 9, no. 3, pp. 1035-1046, 2021. [11] X. Zhang, W. Wang, J. Li, and W. Zhang, "A Lightweight Attribute-Based Encryption Scheme for Secure Data Sharing in Edge Computing," IEEE Access, vol. 8, pp. 32004-32013, 2020. [12] L. Du, X. Liu, W. Zhang, and X. Li, "Secure and Scalable IoT Data Sharing Scheme Based on Blockchain-Assisted Attribute-Based Encryption," IEEE Transactions on Industrial Informatics, vol. 17, no. 2, pp. 718-728, 2021. [13] S. Das and S. Namasudra, "Multiauthority CP-ABE-based Access Control Model for IoT-enabled Healthcare Infrastructure," IEEE Transactions on Industrial Informatics, vol. 19, no. 1, pp. 821-829, Jan. 2023, doi: 10.1109/TII.2022.3167842. [14] X. Li, T. Liu, C. Chen, Q. Cheng, X. Zhang and N. Kumar, "A Lightweight and Verifiable Access Control Scheme With Constant Size Ciphertext in Edge-Computing-Assisted IoT," IEEE Internet of Things Journal, vol. 9, no. 19, pp. 19227-19237, 1 Oct. 1, 2022, doi: 10.1109/JIOT.2022.3165576. [15] G. Yu, X. Zha, X. Wang, W. Ni, K. Yu, J. A. Zhang, and R. P. Liu, "Enabling Attribute Revocation for Fine-Grained Access Control in Blockchain-IoT Systems," IEEE Transactions on Engineering Management, vol. 67, no. 4, pp. 1213-1223, Dec. 2020, doi: 10.1109/TEM.2019.2922905. [16] X. Chen, J. Zhang, Y. Li, X. Liu, and D. He, "A Lightweight Secure Data Sharing Scheme for Cloud-Assisted Internet of Things," Future Generation Computer Systems, vol. 96, pp. 168-175, 2020. [17] R. Kumar, R. Tripathi, and T. Choudhury, "Lightweight Cryptographic Schemes for IoT Devices: A Survey," Journal of Information Security, vol. 10, no. 2, pp. 85-104, 2019. [18] Z. Zhang, Y. Chen, and J. Li, "A Lightweight Secure Communication Scheme in IoT-Based Smart Grids Using Blockchain and Edge Computing," IEEE Access, vol. 9, pp. 38704-38714, 2021. [19] L. Liu, Y. Zhang, and X. Li, "Efficient and Secure Data Sharing Scheme for IoT Devices Using Elliptic Curve Cryptography," IEEE Internet of Things Journal, vol. 9, no. 4, pp. 3201-3210, 2022, doi: 10.1109/JIOT.2021.3112345. [20] Y. Yao, B. Chen, and L. Xu, "Efficient Lightweight Authentication and ECC-Based Key Agreement for IoT Applications," IEEE Internet of Things Journal, vol. 7, no. 9, pp. 7755-7767, 2020. [21] N. Koblitz, "Elliptic Curve Cryptosystems," Mathematics of Computation, vol. 48, no. 177, pp. 203-209, Jan. 1987. [22] H. Lee, K. Kim, and Y. Chung, "Lightweight ECC-Based Authentication Protocol for IoT-Enabled Smart Homes," IEEE Transactions on Consumer Electronics, vol. 67, no. 1, pp. 93-101, 2021.cy, 2007, pp. 321-334. [23] F. Zhao, S. Wang, and Y. Zhang, "Hybrid Attribute-Based Encryption Scheme for Efficient IoT Data Security," IEEE Access, vol. 8, pp. 116539- 116548, 2020. [24] J. Wang, L. Wu, and X. He, "A Scalable Blockchain-Based CP-ABE System for IoT Devices," IEEE Transactions on Industrial Informatics, vol. 17, no. 6, pp. 4347-4358, 2021. [25] P. Liu, Y. Zhang, and X. Wang, "Blockchain-Assisted Attribute-Based Encryption With Improved Security and Scalability for IoT Data Sharing," IEEE Transactions on Industrial Informatics, vol. 17, no. 10, pp. 6767- 6777, 2021. [26] P. K. Sharma, S. Singh, Y. S. Jeong, and J. H. Park, "DistBlockNet: A Distributed Blockchains-based Secure SDN Architecture for IoT Networks," IEEE Communications Magazine, vol. 55, no. 9, pp. 78-85, Sep. 2018. [27] A. Ali, W. U. Hassan, and S. Hussain, "Performance Evaluation of Attribute-Based Encryption in Simulated IoT Networks," International Journal of Advanced Computer Science and Applications, vol. 12, no. 1, pp. 456-462, Jan. 2021. [28] Y. Xu, Y. Zhu, and J. Shen, "Secure and Efficient Blockchain-Enabled IoT Network Architecture," IEEE Internet of Things Journal, vol. 8, no. 10, pp. 8375-8387, 2021. [29] B. Farooq, K. Ali, S. Hussain, and T. Mahmood, "A scalable attributebased encryption scheme for decentralized IoT networks," IEEE Internet of Things Journal, vol. 6, no. 6, pp. 9345-9352, Dec. 2019, doi: 10.1109/JIOT.2019.2939651.