



Enhancing IoT Security by Multi-Factor Authentication with Blockchain: Methods and Applications

Abdulla J. Y. Aldarwish^{1,3}, Kalyani Patel², Aqeel A. Yaseen¹, Ali A. Yassin³

¹Department of Computer Science, Gujarat University, Ahmedabad, 380009, India.

²K.S. School of Business Management and Information Technology, Gujarat University, Ahmedabad, India,

³Department of Computer Sciences, Education College for Pure Sciences, University of Basrah, 6100, Iraq.

Corresponding Author- Abdulla J. Y. Aldarwish

Email- abdullajas@gmail.com

Abstract:

The Internet of Things (IoT) has transformed device interaction, enhancing automation and efficiency. However, the surge in connected devices poses significant security challenges, especially regarding data integrity and confidentiality. Traditional single-factor authentication (SFA) methods are inadequate against advanced cyber threats, requiring more robust security measures. This paper integrates Multi-Factor Authentication (MFA) with blockchain technology to create a secure, scalable, and efficient authentication framework for IoT environments. Leveraging blockchain's decentralized and immutable features with lightweight cryptographic techniques, this approach mitigates risks of unauthorized access and data breaches. The study addresses IoT devices' computational constraints, scalability issues, and privacy concerns, offering innovative solutions and practical applications. Real-world case studies in smart homes, industrial IoT, healthcare, supply chains and smart cities are presented. Future research directions are also suggested to enhance IoT security with MFA and blockchain.

Keyword: authentication, ECC, blockchain, Internet of Things, MFA

Introduction:

The Internet of Things (IoT) has fundamentally transformed device interactions, fostering unprecedented levels of automation and operational efficiency across diverse sectors. However, the rapid proliferation of connected devices introduces significant security challenges. Ensuring the integrity and confidentiality of data within IoT environments is paramount, given the limited computational resources and widespread distribution of these devices (Bamashmos et al., 2024; Wanisha et al., 2024).

Traditional IoT authentication methods, such as single-factor authentication (SFA), have proven inadequate against sophisticated cyber threats. These methods leave both devices and users vulnerable to attacks, including man-in-the-middle, impersonation, and replay attacks (Al Hwaitat et al., 2023; Wanisha et al., 2024). Multi-Factor Authentication (MFA) has emerged as a robust method to enhance IoT security by providing additional layers of protection beyond traditional password-based systems. Blockchain technology, known for its decentralized and immutable characteristics, offers a promising solution to address various security concerns inherent in IoT networks (Ahsan et al., 2022).

This paper aims to explore the integration of MFA and blockchain technologies to develop a secure, scalable, and efficient authentication

framework tailored to the unique requirements of IoT devices. By leveraging blockchain's capabilities to create a tamper-proof and transparent authentication system, this approach significantly reduces the risk of unauthorized access and data breaches (Panda et al., 2021; Syahrina et al., 2024).

Objectives and Contributions:

- 1. Enhance IoT Security:** Investigate how MFA can bolster security in IoT environments by using multiple authentication factors beyond passwords.
- 2. Integrate Blockchain Technology:** Explore the application of blockchain in MFA for IoT, leveraging its decentralized and immutable properties for a robust authentication system.
- 3. Address Current Challenges:** Identify and address major challenges in implementing MFA in IoT, including computational constraints, scalability, and privacy concerns.
- 4. Propose Innovative Solutions:** Develop novel methods combining MFA with blockchain and lightweight cryptographic techniques tailored for IoT devices.
- 5. Showcase Practical Applications:** Demonstrate practical implementation through real-world applications and case studies, illustrating the effectiveness and efficiency of the proposed solutions.

By leveraging MFA and blockchain technologies, this paper aims to develop a secure, scalable, and

efficient authentication framework for IoT devices, offering valuable insights for researchers and practitioners.

Related Work:

Multi-Factor Authentication (MFA) has become a cornerstone for enhancing security in IoT environments. MFA leverages multiple authentication factors to provide a higher level of security compared to single-factor solutions. The integration of MFA into IoT systems addresses the inherent vulnerabilities associated with single-factor authentication mechanisms, such as password-only systems, which are susceptible to a wide range of cyber-attacks (Cui et al., 2024).

Blockchain technology offers a decentralized and immutable ledger system, which is highly effective for authentication purposes. Several studies have explored its application in IoT security. For instance, Fedorov et al. proposed a blockchain-based device authentication method specifically designed for the Industrial Internet of Things (IIoT). This method significantly enhances security by providing a robust access point for IoT devices against unauthorized access and data forgery (Al Hwaitat et al., 2023). However, challenges remain, particularly in balancing security with the computational and power constraints of IoT devices (Zargar et al., 2024).

Incorporating lightweight authentication schemes in IoT is crucial due to the limited computational resources of many IoT devices. Ismail et al. presented a lightweight identity management system that combines blockchain technology with machine learning to detect denial-of-service threats, thus improving overall system security (Ismail et al., 2024). Despite these advancements, the integration of blockchain into IoT networks can strain communication and memory resources, necessitating a balance between security and performance (Wang et al., 2022).

Recent advancements have seen the integration of deep learning with blockchain to bolster IoT security. Singh et al. introduced a deep-learning-based intrusion detection system combined with a private blockchain to secure IIoT environments. This framework effectively acts as a defense mechanism against cyber-attacks but faces issues such as high computational complexity and adaptability (Singh et al., 2024).

Cui et al. proposed a blockchain-based cross-domain authentication management system for IoT devices. This system ensures secure device management across different domains by leveraging blockchain's decentralized nature and the Merkle tree structure for storing confidential information. The system's strength lies in its low on-chain storage requirements and rapid off-chain authentication processes (Cui et al., 2024).

Challenges in Implementing MFA in IoT with Blockchain:

Implementing Multi-Factor Authentication (MFA) in IoT environments with blockchain integration presents several challenges.

- 1. Computational Constraints of IoT Devices:** IoT devices often have limited computational power, memory, and energy resources, making it difficult to perform resource-intensive blockchain and cryptographic operations. Lightweight cryptographic techniques and optimized blockchain protocols are essential to address these limitations (Ahsan et al., 2022).
- 2. Scalability and Network Latency Issues:** Blockchain's decentralized consensus and data immutability can increase network latency and reduce transaction throughput. As the number of IoT devices grows, scalability and latency issues worsen. Solutions like sharding, off-chain transactions, and Layer 2 solutions can help mitigate these problems (Wanisha et al., 2024).
- 3. Usability and User Experience Considerations:** Balancing security and usability is critical. MFA mechanisms can be cumbersome and negatively impact user experience. Ensuring a seamless, user-friendly authentication process while maintaining robust security is crucial (Wanisha et al., 2024).
- 4. Privacy and Data Protection Concerns:** Blockchain's transparency and immutability can pose privacy challenges. Storing authentication data on a public ledger may expose sensitive information. Techniques such as zero-knowledge proofs, homomorphic encryption, and private blockchains can enhance privacy while leveraging blockchain's security benefits (Sharma et al., 2023).

Addressing these challenges is essential for developing secure, scalable, and user-friendly authentication solutions for IoT systems.

Proposed Methods:

Leveraging Blockchain for Decentralized Authentication:

Blockchain technology provides a decentralized, immutable, and transparent ledger system to enhance IoT authentication security. It eliminates single points of failure in centralized systems, reducing risks like man-in-the-middle attacks and data tampering. IoT devices register on the blockchain network, and authentication requests are processed through self-executing smart contracts that verify identities by cross-referencing stored information. This decentralized method ensures no single entity controls the entire authentication process, enhancing security and trust (Ahsan et al., 2022).

Lightweight Cryptographic Techniques for IoT:

Lightweight cryptographic techniques are essential for IoT devices with limited computational

resources. These techniques ensure security without overburdening devices. Elliptic curve cryptography (ECC) offers comparable security to traditional methods with smaller key sizes, resulting in faster computations and lower power consumption. Lightweight hash functions like SHA-256 and SHA-3 ensure data integrity and authenticity. By optimizing cryptographic algorithms for IoT, robust security is maintained while preserving device resources (Panda et al., 2021).

Fog Computing to Offload Processing Tasks:

Fog computing brings computational resources closer to data sources, beneficial for IoT environments with latency and bandwidth limitations. Offloading tasks to fog nodes reduces the burden on IoT devices and improves system efficiency. In our method, fog nodes handle resource-intensive blockchain and cryptographic operations, acting as intermediaries to process authentication requests and verify transactions before recording them on the blockchain. This enhances system performance, scalability, and security by distributing tasks across multiple nodes (Wanisha et al., 2024).

Combining MFA with Blockchain: Architecture and Workflow:

The integration of Multi-Factor Authentication (MFA) with blockchain technology provides a robust and scalable solution for securing IoT environments. The proposed architecture consists of the following components:

1. **IoT Devices:** These devices initiate authentication requests and interact with fog nodes and blockchain networks.
2. **Fog Nodes:** Acting as intermediaries, fog nodes process authentication requests, perform cryptographic operations, and communicate with the blockchain network.
3. **Blockchain Network:** A decentralized ledger that stores authentication data, executes smart contracts, and verifies transactions.

Workflow:

1. **Registration:** IoT devices and users are registered on the blockchain network, with their identity and authentication data stored securely using cryptographic techniques.
2. **Authentication Request:** When an IoT device initiates an authentication request, it sends the request to the nearest fog node.
3. **MFA Verification:** The fog node verifies the first authentication factor (e.g., password) and then requests additional factors (e.g., biometric data, OTP) from the user.
4. **Blockchain Verification:** Once all authentication factors are verified, the fog node communicates with the blockchain network to execute a smart contract that validates the user's identity and grants access.

5. **Access Grant:** Upon successful verification, the fog node grants access to the IoT device, and the transaction is recorded on the blockchain for audit and tracking purposes.

This architecture ensures that authentication is both decentralized and multi-layered, providing enhanced security and scalability for IoT environments.

Applications and Case Studies

Smart Home Automation:

Integrating Multi-Factor Authentication (MFA) with blockchain in smart home automation enhances security and convenience. Each IoT device, like smart locks and cameras, is registered on a blockchain network. Users authenticate using MFA, such as a password and biometric scan, before accessing devices. A fog node processes the request, verifies credentials, and communicates with the blockchain to validate identity. Successful verification grants access and records the transaction on the blockchain.

Outcomes: This approach ensures only authorized users control devices, provides a tamper-proof access record, and enhances resilience against cyber-attacks by eliminating single points of failure (Ahsan et al., 2022).

Industrial IoT (IIoT) for Manufacturing:

Integrating MFA with blockchain in manufacturing enhances security, prevents unauthorized access, and ensures data integrity.

Implementation: IoT sensors and actuators are deployed on a blockchain network, requiring MFA for access. Maintenance personnel use RFID badges and biometric data to access control panels. Fog nodes verify credentials and interact with the blockchain to confirm identity. Authenticated personnel perform tasks, with all actions logged on the blockchain.

Outcomes: This ensures only authorized personnel access critical systems, reduces sabotage risks, and provides a tamper-proof activity record, facilitating regulatory compliance and enhancing IIoT infrastructure security and reliability (Zhang et al., 2023).

Healthcare Systems:

Integrating MFA with blockchain in healthcare enhances data security and controls access to medical devices.

Implementation: Medical IoT devices, like patient monitors and infusion pumps, are integrated into a blockchain network. Healthcare providers authenticate using smart cards and biometric verification to access patient data and control devices. Fog nodes process these requests, verify credentials, and validate identity through the blockchain before granting access.

Outcomes: This approach ensures only authorized personnel access medical devices, enhancing patient data security and compliance with regulations. The immutable blockchain ledger improves

accountability and helps prevent data breaches and unauthorized access, protecting patient privacy and safety (Islam et al., 2019).

Smart Cities:

Integrating MFA with blockchain secures critical infrastructure in smart cities, such as traffic management, energy grids, and public safety networks.

Implementation: IoT devices managing city infrastructure are registered on a blockchain network. Authorized personnel use MFA to access and control these systems, with fog nodes handling authentication and blockchain verification.

Outcomes: This ensures only authorized individuals manage city infrastructure, enhancing security and reliability. The blockchain provides a transparent access record, improving accountability and resource management. The decentralized blockchain reduces the risk of systemic failures and cyber-attacks on city infrastructure (Tareen et al., 2023).

The integration of MFA with blockchain technology in IoT environments offers significant enhancements in security, transparency, and reliability across various applications. From smart homes and industrial settings to healthcare, supply chain management, and smart cities, this approach addresses critical security challenges and provides robust solutions for real-world implementations.

Conclusion and Future Work:

This paper explored integrating Multi-Factor Authentication (MFA) with blockchain technology to enhance IoT security. Key discussions included using blockchain for decentralized authentication, employing lightweight cryptographic techniques for IoT devices, offloading tasks via fog computing, and creating a robust authentication framework. Practical scenarios were demonstrated in domains such as smart home automation, industrial IoT, healthcare, supply chain management, and smart cities.

Combining MFA with blockchain significantly improves IoT security by addressing critical challenges. Decentralized authentication enhances resilience against cyber-attacks, eliminating single points of failure. Lightweight cryptographic techniques maintain operational efficiency without overburdening IoT devices. Fog computing optimizes performance and scalability by distributing computational load. This multi-layered security framework protects against unauthorized access and ensures data integrity and transparency through blockchain's immutable nature.

Future Research Directions and Potential Improvements

While promising, the proposed methods require further research for full potential realization:

1. Optimization of Lightweight Cryptographic Algorithms
2. Scalability Solutions for Blockchain

3. Enhanced Privacy Mechanisms
4. Interoperability Standards
5. Energy-Efficient Solutions
6. Real-World Testing and Validation
7. Regulatory and Compliance Frameworks

The integration of MFA with blockchain presents a robust solution to IoT security challenges. This approach enhances security, scalability, and efficiency by combining decentralized authentication, lightweight cryptographic techniques, and fog computing. Ongoing research and development are essential to address remaining challenges and optimize solutions for real-world applications, further strengthening IoT security and creating more reliable ecosystems.

References:

1. Ahsan, T., Zeeshan Khan, F., Iqbal, Z., Ahmed, M., Alroobaea, R., Baqasah, A. M., Ali, I., & Raza, M. A. (2022). IoT Devices, User Authentication, and Data Management in a Secure, Validated Manner through the Blockchain System. *Wireless Communications and Mobile Computing*, 2022. doi: 10.1155/2022/8570064
2. Al Hwaitat, A. K., Almaiah, M. A., Ali, A., Al-Otaibi, S., Shishakly, R., Lutfi, A., & Alrawad, M. (2023). A New Blockchain-Based Authentication Framework for Secure IoT Networks. *Electronics (Switzerland)*, 12(17). doi: 10.3390/electronics12173618
3. Bamashmos, S., Chilamkurti, N., & Shahraki, A. S. (2024). Two-Layered Multi-Factor Authentication Using Decentralized Blockchain in an IoT Environment. *Sensors*, 24(11). doi: 10.3390/s24113575
4. Cui, J., Zhu, Y., Zhong, H., Zhang, Q., Gu, C., & He, D. (2024). Efficient blockchain-based mutual authentication and session key agreement for cross-domain IIoT. *IEEE Internet of Things Journal*.
5. Islam, N., Faheem, Y., Din, I. U., Talha, M., Guizani, M., & Khalil, M. (2019). A blockchain-based fog computing framework for activity recognition as an application to e-Healthcare services. *Future Generation Computer Systems*, 100, 569–578.
6. Ismail, S., Nouman, M., Dawoud, D. W., & Reza, H. (2024). Towards a lightweight security framework using blockchain and machine learning. *Blockchain: Research and Applications*, 5(1), 100174.
7. Panda, S. S., Jena, D., Mohanta, B. K., Ramasubbareddy, S., Daneshmand, M., & Gandomi, A. H. (2021). Authentication and Key Management in Distributed IoT Using Blockchain Technology. *IEEE Internet of Things Journal*, 8(16), 12947–12954. doi: 10.1109/JIOT.2021.3063806

8. Sharma, P. C., Mahmood, M. R., Raja, H., Yadav, N. S., Gupta, B. B., & Arya, V. (2023). Secure authentication and privacy-preserving blockchain for industrial internet of things. *Computers and Electrical Engineering*, 108, 108703.
9. Singh, S., Chhabra, R., & Arora, J. (2024). A systematic review of waste management solutions using machine learning, Internet of Things and blockchain technologies: state-of-art, methodologies, and challenges. *Archives of Computational Methods in Engineering*, 31(3), 1255–1276.
10. Syahrina, N., Juni, B., Juni¹, B., Wan¹, G. H., Aisyah, S., Binti Banchi¹, N., Blessings, E., Bajau¹, A., Loganathan¹, V. A. / P., & Faisal², M. (2024). Advancements in Multi-Factor Authentication: A Quantum-Resilient and Federated Approach for Enhanced Security. *International Journal of Computer Technology and Science*, 3, 71–86. doi: 10.62951/ijcts.v1i3.26
11. Tareen, F. N., Alvi, A. N., Malik, A. A., Javed, M. A., Khan, M. B., Saudagar, A. K. J., Alkhathami, M., & Abul Hasanat, M. H. (2023). Efficient load balancing for blockchain-based healthcare system in Smart Cities. *Applied Sciences*, 13(4), 2411.
12. Wang, J., Chen, J., Ren, Y., Sharma, P. K., Alfarraj, O., & Tolba, A. (2022). Data security storage mechanism based on blockchain industrial Internet of Things. *Computers & Industrial Engineering*, 164, 107903.
13. Wanisha, I., Bravyain, J., Silas, J., Hakim Bin Mohammad Bakery, L., Samuel, M., & Faisal, M. (2024). Multi-Factor Authentication Using Blockchain: Enhancing Privacy, Security and Usability. *International Journal of Computer Technology and Science*, 3, 41–55. doi: 10.62951/ijcts.v1i3.24
14. Zargar, G. R., Barati, H., & Barati, A. (2024). An authentication mechanism based on blockchain for IoT environment. *Cluster Computing*, 1–17.
15. Zhang, F., Wang, H., Zhou, L., Xu, D., & Liu, L. (2023). A blockchain-based security and trust mechanism for AI-enabled IIoT systems. *Future Generation Computer Systems*, 146, 78–85.