EPJ Web of Conferences **380**, 02015 (2026) https://doi.org/10.1051/epjconf/202638002015
ICISCT'25

A Multi-Factor Authentication Framework for IoT Healthcare Systems Based on Blockchain and Smart Contract

Chaimae El Filali[1,*], *Imad* Bourian[1,†], and *Khalid* Chougdali[1,‡]

[1]National School of Applied Sciences, Ibn Tofail University, Kenitra, Morocco

Abstract. Authentication is becoming essential due to the expansion of the Internet of Things (IoT) applications in smart cities, supply chain, and healthcare. In the healthcare sector, hospitals use centralized server-based systems to manage user information and patient medical records. However, this approach may lead to scalability, interoperability, security and privacy challenges. To address these issues, this paper presents a blockchain-based multi-factor authentication (MFA) framework for IoT healthcare systems. The framework uses the Ethereum blockchain and smart contracts to improve authentication security and minimize unauthorized access risk. It also uses the InterPlanetary File System (IPFS) to securely and efficiently store sensitive medical data. Performance and security are evaluated to show the effectiveness, reliability, and feasibility of the proposed system.

1 Introduction

The healthcare sector is essential for the well-being of a nation, and recent technological developments have supported the use of digital healthcare systems to improve the quality of medical services and the availability of healthcare information [1]. However, the increase in security breaches and privacy violations has raised significant concerns about network security, making the protection of sensitive data crucial.

This study highlights the need for robust security mechanisms to address existing vulnerabilities. Satoshi Nakamoto introduced blockchain in 2008, which is a decentralized peer-to-peer network that securely records transaction histories and ensures data integrity and tamper-proof sharing [2]. Blockchain is an open-source system that allows users to contribute and access a distributed database, which uses asymmetric encryption and consensus mechanisms for transaction validation without a central authority [3]. In the changing healthcare sector, blockchain can enhance user data protection and access control, which enables secure interactions among patients and medical staff [4].

Authentication is important for verifying the identities of users seeking access, which ensures that only properly identified entities can access organizational systems. Many organizations have recently adopted access control techniques to strengthen security, which focus on identity authorization and authentication. MFA further improves security by verifying the identity of users through two or more independent authentication factors, including passwords, one-time passwords (OTP), and biometrics [5].

*e-mail: chaimae.elfilali@uit.ac.ma
†e-mail: imad.bourian@uit.ac.ma
‡e-mail: khalid.chougdali@uit.ac.ma

Secure storage of sensitive data also represents a significant challenge in healthcare. Decentralized storage solutions such as IPFS offer an alternative to centralized models [6]. IPFS enhances reliability, privacy, and interoperability for IoT applications, by storing and retrieving data through a distributed network of nodes. As a result, sensitive medical data is better protected while still being accessible when needed.

The proposed framework uses Ethereum blockchain and IPFS to provide secure authentication and data management in IoT healthcare systems. Ethereum is used to manage user identities, authentication requests, and access permissions through smart contracts, while sensitive medical records are stored off-chain using IPFS to reduce blockchain storage overhead. Authentication is improved using the MFA mechanism that requires multiple verification factors before access is granted. This approach reduces unauthorized access risk when one authentication factor is compromised. Authentication and access control are implemented using Solidity smart contracts, providing secure and immutable IoT authentication without relying on centralized servers [7]. The Advanced Encryption Standard (AES) is used to protect sensitive medical information before it is stored on IPFS. This additional encryption layer improves confidentiality while leveraging the availability and resilience of decentralized storage [8].

The paper is organized as follows: Section 2 introduces the problem statement. Section 3 provides related work. Section 4 presents the proposed architecture. Section 5 explains the implementation and the technologies used. Section 6 evaluates performance and security. Finally, Section 7 concludes the paper.

2 Problem Statement

The rapid growth of IoT applications has increased the need for secure device authentication and user protection. Existing IoT systems still rely on single-factor authentication (SFA) or two-factor authentication (2FA) that can be vulnerable to advanced cyber threats, exposing both devices and users to various attacks [9].

This study develops an MFA system integrated with decentralized blockchain technology for IoT environments. The system is designed to:

- Improve security: Use multiple authentication factors to minimize unauthorized access risk.
- Respect privacy: Minimize data collection and protect user anonymity.
- Emphasize usability: Offer user-friendly authentication methods to support legitimate access.

2.1 Overview of Secured IoT Healthcare Systems

The IoT is important for improving efficiency and accessibility in healthcare. However, robust security and patient privacy are paramount concerns that can only be addressed with strict measures [10]. Implementing MFA and blockchain for user authentication, along with IPFS and AES for secure data storage and encryption, creates a strong protective barrier against unauthorized access. This decentralized blockchain network also securely stores authentication details, allowing access to connected data and devices only after successful authentication.

3 Related Work

Blockchain technology is increasingly used in authentication systems. For instance, "AuthChain," as discussed in [11], is a decentralized solution that reduces risks from centralized providers vulnerable to hacks. AuthChain improves online user authentication security and reduces data breach risks by using Distributed Ledger Technology (DLT). However, a privacy-preserving approach is necessary to avoid storing user information as plain text on the blockchain. In [12], the authors explored security vulnerabilities in metaverse platforms like Roblox and Fortnite, proposing a blockchain-based model for secure communication. This model used ECC and biometric data for mutual authentication, showing resilience to threats. In contrast, [13] addressed centralized authentication issues in the metaverse, such as impersonation and server spoofing, by introducing a blockchain-enabled architecture to authenticate avatars. However, it relies on a centralized authority, creating a single point of failure. Although [13] aims to ensure privacy through the blockchain, the data on the blockchain remain accessible without additional privacy mechanisms.

In [14], the authors critiqued traditional username and password systems and present "BAuth-ZKP," a blockchain-based multi-factor authentication method using smart contracts and zero-knowledge proofs for secure transactions in smart cities, although ZKP details are limited. Additionally, [15] proposed integrating blockchain with multi-factor authentication to enhance trust in IoT domains, encoding multiple authentication factors using hardware fingerprints. However, this approach also depends on a single trusted authority per domain which poses a potential risk.

4 Proposed Solution

This section introduces our solution that uses blockchain and smart contracts to create a secure and decentralized authentication and access control system. This approach addresses privacy concerns by eliminating the reliance on a central authority and reducing the risks associated with weak passwords in IoT applications. Our solution incorporates an MFA scheme that leverages the decentralized trust of smart contracts and blockchain technology.

4.1 System design

Our system consists of five primary components. Figure 1 shows our authentication scheme and the associated processes.

1. **Blockchain** : Serves as a secure and immutable ledger for storing user information and access permissions. This ensures transparency, prevents unauthorized modifications, and enables traceability of data access, which foster trust among all parties involved in the healthcare system.

2. **IPFS** : A decentralized storage system that distributes encrypted healthcare data across multiple nodes. It improves redundancy and ensures continuous access to critical information. Healthcare data is encrypted using AES-128, a highly secure algorithm, to protect sensitive information from unauthorized access.

3. **Smart contract** : Deployed on the Ethereum blockchain to implement MFA and manage user access to data. These smart contracts authenticate users and interact with data stored on IPFS, which ensure a secure and transparent user verification without a central authority.

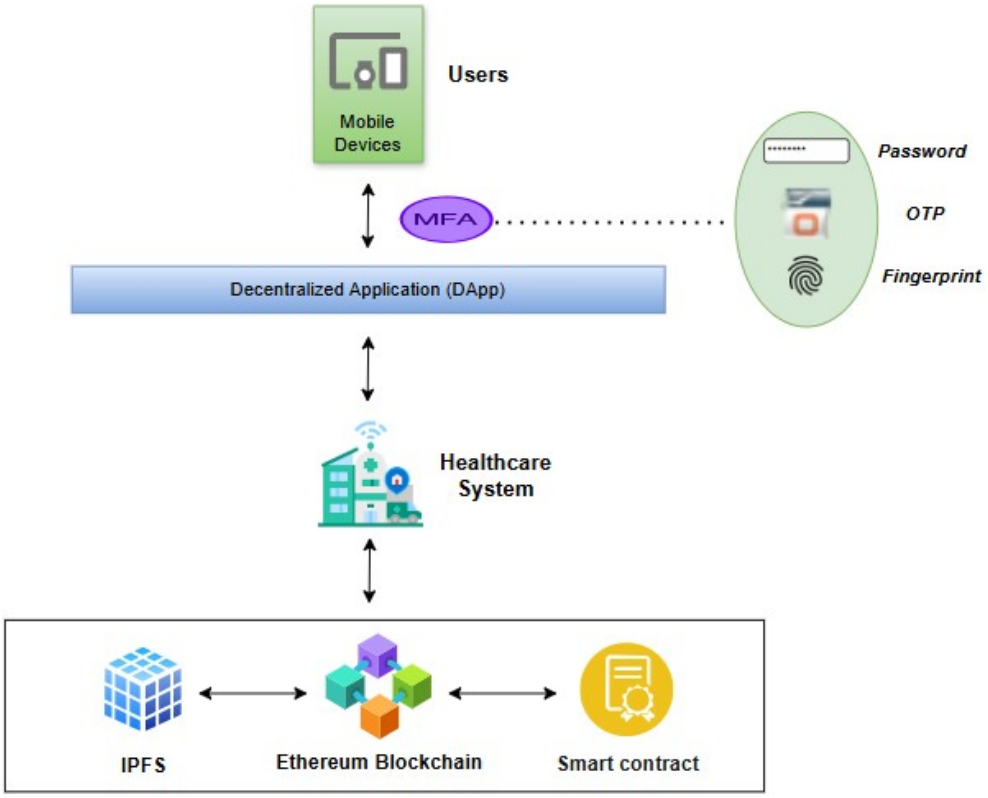


Figure 1: The proposed MFA architecture for IoT healthcare systems

4. **Healthcare system** : Consists of IoT-based devices like temperature and blood sensors. These sensors collect health metrics, format them, and associate the data with patient accounts.

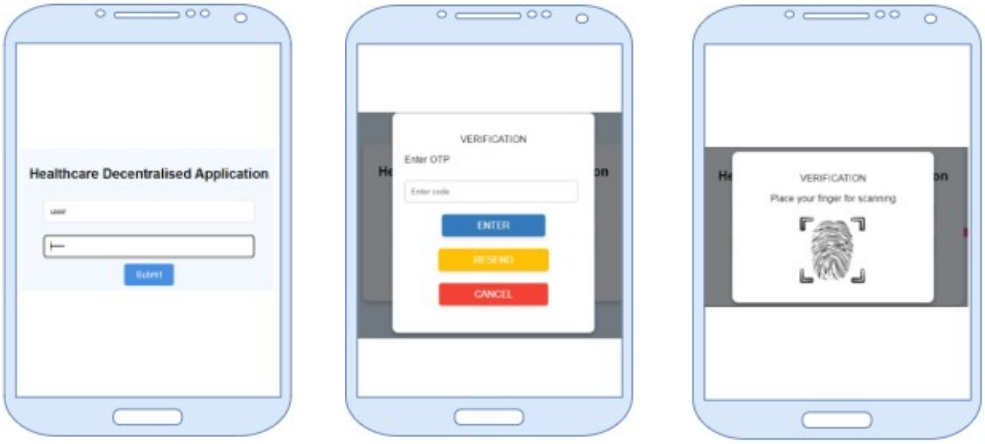
5. **DApp** : Provides a user-friendly interface that simplifies the authentication process. Users start by creating an account, registering with an e-mail address and password, then verify their identity via OTP as the second authentication factor, and fingerprint biometrics as the third authentication factor.

4.2 System workflow

The workflow of our approach begins with user registration and identity verification via a DApp. New users initiate the process by setting up MFA options, including passwords, OTPs, and biometrics. Their information, authentication methods, and chosen roles are securely stored on the blockchain.

When a user requests an OTP for the login, the blockchain generates it and records the timestamp and expiration. As shown, Figure 2, user first enters the password. If correct, an OTP is sent to his e-mail address, which must be entered alongside the most recent one. The final authentication step is the biometric verification using fingerprints.

Sensitive data, such as patient records and lab results, are encrypted using AES to ensure confidentiality. The encryption keys are securely managed so that only authorized users can



(a) First step (b) Second step (c) Third step

Figure 2: Authentication process through three consecutive steps

decrypt the data. The encrypted data are then uploaded to IPFS, where a unique content hash is generated for secure retrieval. This content hash and metadata, including access permissions, are stored on the blockchain to ensure integrity and traceability.

Access control is implemented through smart contracts that define permissions based on user roles, such as doctor or nurse, allowing users to access only the data necessary for their functions. After successful authentication, users can request specific encrypted data, which are retrieved and decrypted using the IPFS secure encryption key.

5 Implementation

This section describes the technologies used and how our system is implemented. The model contains the smart contract component and the decentralized web application component.

5.1 Smart contract implementation

We developed our framework on the Ethereum blockchain for its efficient support and smart contract capabilities. Using Solidity, we created four main contracts: **UserManage** for user registration and roles, **AccessManage** for managing permissions to data based on user roles, **DataManage** for encrypted data storage and retrieval from IPFS, and **mfaManage** for multi-factor authentication setup and verification. These contracts were compiled with Hardhat and deployed using the Ethereum Virtual Machine (EVM) on the local Hardhat network.

5.2 Decentralized web app

Our proposed architecture includes a DApp with front-end and back-end interfaces. The front-end is accessible via mobile apps and is designed using HTML5 and CSS. The back-end is built with JavaScript and uses Web3 technology to connect users to the decentralized network and access the data. The DApp communicates with the EVM through Remote Procedure Calls (RPC), instantiating a new Web3 instance using the Ethereum blockchain address.

Smart contracts are invoked through their Application Binary Interface (ABI) and contract address, which allow interactions with blockchain nodes via defined functions.

6 Results and Discussions

This section presents the evaluation results of the performance of the proposed MFA system. The evaluation was run on Windows 10, using an Intel Core i5 processor and 8 GB of RAM. A series of experimental tests were performed using different performance metrics to provide in-depth analysis.

6.1 System performance

As shown in Figure 3–6, we evaluated performance using metrics such as CPU consumption, memory usage, processing time, and the cost of deploying smart contracts on the Ethereum network. The analysis shows that the **mfaManage** contract performs the best on all measured metrics, which results in the lowest deployment cost (0.000245392 ETH), the shortest execution time (65 ms), the least memory consumption (4.30 MB), and minimal CPU usage (11.53%). This highlights that **mfaManage** is feasible for real-time authentication workflows, especially in resource-constrained environments such as IoT medical devices. Next, the **UserManage** contract has the highest memory usage (30.79 MB) and the longest execution latency (146 ms), because it manages user identities and registrations. However, its CPU usage (14.65%) and gas cost (0.000424866 ETH) remain acceptable for decentralized deployment. The **AccessManage** contract has higher CPU consumption (20.00%), but moderate execution time (98 ms) and memory usage (12.11 MB) because of its role in enforcing dynamic access policies. Finally, the **DataManage** contract has a balanced performance across all categories, with the highest CPU usage of 27.46% because of data integrity verification and storage operations.

Figure 7 shows that the main factors affecting the smart contract deployment cost in ETH are the gas consumption and gas price. Gas consumption depends on computational complexity, storage requirements, and interactions between contracts, while gas price fluctuates according to network conditions such as congestion and mining activity. For example, the **AccessManage** contract has the highest deployment cost (0.00048134 ETH) due to the additional processing for permission verification and enforcement in role-based access control.

The obtained results show that the proposed framework is feasible for the secure authentication in IoT healthcare systems. Blockchain, smart contracts, and IPFS are used to manage data efficiently and to reduce the dependence on centralized infrastructures. In addition, storing medical data on IPFS reduces blockchain storage overhead and supports more efficient access to sensitive information.

6.2 Security analysis

1. Blockchain-Based MFA: The use of blockchain and smart contracts in the MFA process reinforces security by providing decentralized control in our system. This ensures immutability, transparency, and automated enforcement of security policies. It also reduces reliance on third-party providers, gives users better control over authentication data, and provides a reliable audit trail. In addition, it improves resilience to phishing and replay attacks and allows for trustworthy and scalable authentication.

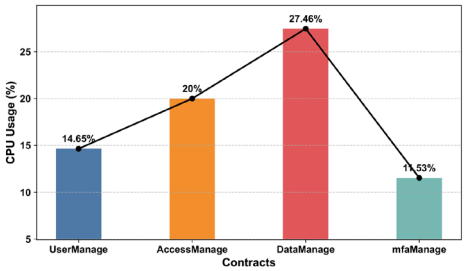


Figure 3: CPU consumption

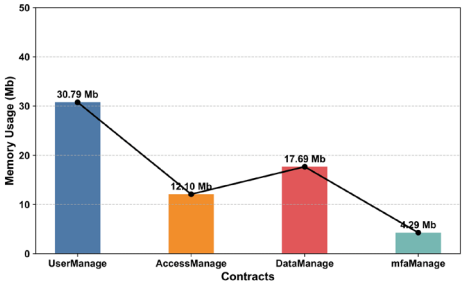


Figure 4: Memory consumption

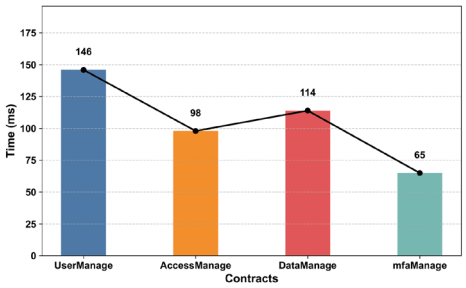


Figure 5: Time consumption

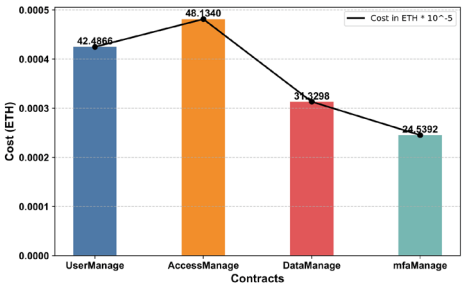


Figure 6: Deployment cost

2. Unauthorized Access: Access controls restrict users to only the data required for their roles. Permissions are stored on the blockchain to prevent unauthorized access to sensitive information. As a result, it reduces the risk of data breaches and Man-in-the-Middle (MitM) attacks and ensures that only authorized users can view or modify data.

3. Data privacy: Sensitive medical data is encrypted using AES and stored on IPFS rather than being stored directly on the blockchain. This improves storage efficiency, reduces costs, and increases scalability. Even if data is accessed, it remains unreadable without the appropriate decryption keys.

4. Denial of Service (DoS) Attacks: The distributed nature of blockchain and IPFS enhances availability and eliminates single points of failure, reducing the risk of service disruption caused by attackers.

6.3 Security comparison

Table 1 compares the security features of our proposed system with three related studies, which highlight resilience against various cyber threats. Our findings show that our system is robust against DoS, replay, MitM, and data tampering attacks, in contrast to related studies.

7 Conclusion

Digital healthcare requires strong security measures to protect sensitive information. This research introduces a secure healthcare authentication system that utilizes blockchain technology and smart contracts to manage the MFA process and enhance user identity verification.

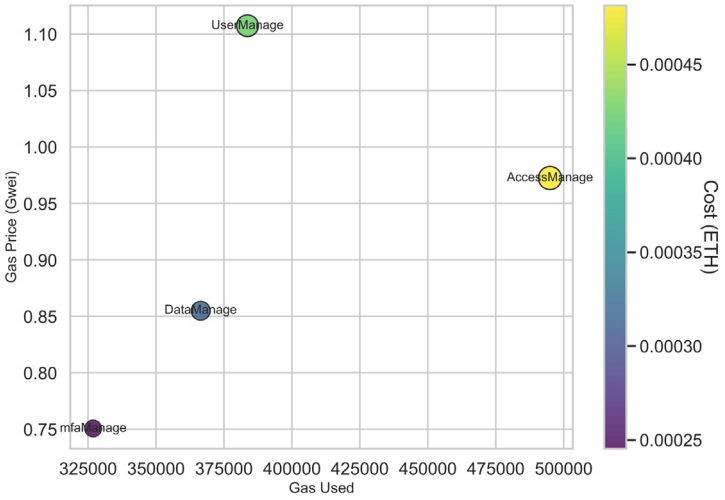


Figure 7: Cost analysis based on gas used and gas price

Table 1: Security comparison with related work

Security Feature	[12]	[13]	[15]	**Proposed Framework**
Replay attack resilience	✓	✓	✓	✓
DoS attack resilience	×	✓	×	✓
MitM attack resilience	✓	×	×	✓
Data tampering resilience	×	×	✓	✓

By removing third-party involvement, we foster user trust, and create a path for future secure healthcare solutions. We also use IPFS to store AES-encrypted data which ensures efficient and confidential handling. Our system reliably authenticates users while protecting against attacks such as DoS, replay, MitM, and data tampering. Future work will address the use of email for OTP delivery by exploring more secure alternatives, such as authenticator apps, and assess the system's effectiveness in real-world environments.

References

[1] M. Paul, L. Maglaras, M. A. Ferrag, I. Almomani, Digitization of healthcare sector: A study on privacy and security concerns. ICT Express **9**, 571–588 (2023). https://doi.org/10.1016/j.icte.2023.02.007

[2] Q. Wang, Y. Liu, Blockchain for public safety: A survey of techniques and applications. J. Saf. Sci. Resil. (2023). https://doi.org/10.1016/j.jnlssr.2023.09.001

[3] G. Tripathi, M. A. Ahad, G. Casalino, A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges. Decis. Anal. J. **8**, 100344 (2023). https://doi.org/10.1016/j.dajour.2023.100344

[4] A. Haleem, M. Javaid, R. P. Singh, R. Suman, S. Rab, Blockchain technology applications in healthcare: An overview. Int. J. Intell. Netw. **2**, 130–139 (2021). https://doi.org/10.1016/j.ijin.2021.09.005

[5] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, Y. Koucheryavy, Multi-factor authentication: A survey. Cryptography **2**(1), 1 (2018). https://doi.org/10.3390/cryptography2010001

[6] B. K. Mohanta, S. S. Panda, D. Jena, An overview of smart contract and use cases in blockchain technology. In: Proc. 9th Int. Conf. Comput. Commun. Netw. Technol. (ICCCNT), 1–4 (2018). https://doi.org/10.1109/ICCCNT.2018.8494045

[7] I. Bourian, A. Sebbar, M. Arioua, K. Chougdali, Blockchain-based smart contract to enhance security in smart city. In: Proc. 11th Int. Conf. Wireless Netw. Mobile Commun. (WINCOM), 1–6 (2024). IEEE. https://doi.org/10.1109/WINCOM62286.2024.10657758

[8] C. El Filali, I. Bourian, K. Chougdali, Privacy-preserving and access control scheme for Internet of Things-based healthcare systems using Ethereum blockchain. In: Proc. 7th Int. Conf. Adv. Commun. Technol. Netw. (CommNet), 1–6 (2024). IEEE. https://doi.org/10.1109/CommNet63022.2024.10793370

[9] T. Suleski, M. Ahmed, W. Yang, E. Wang, A review of multi-factor authentication in the Internet of Healthcare Things. Digital Health **9** (2023). https://doi.org/10.1177/20552076231177144

[10] S. Abdulmalek, A. Nasir, W. A. Jabbar, M. A. Almuhaya, A. K. Bairagi, M. A. M. Khan, S. H. Kee, Internet of Things-based healthcare monitoring system towards improving quality of life: A review. Healthcare **10**(10), 1993 (2022). https://doi.org/10.3390/healthcare10101993

[11] S. Y. Lim, P. T. Fotsing, O. Musa, A. Almasri, AuthChain: A decentralized blockchain-based authentication system. Int. J. Eng. Trends Technol. **70**, 70–74 (2020). https://doi.org/10.14445/22315381/CATI1P212

[12] J. Ryu, S. Son, J. Lee, Y. Park, Y. Park, Design of secure mutual authentication scheme for metaverse environments using blockchain. IEEE Access **10**, 98944–98958 (2022). https://doi.org/10.1109/ACCESS.2022.3206457

[13] S. Patwe, S. Mane, Blockchain-enabled architecture for secure authentication in the metaverse environment. In: Proc. IEEE 8th Int. Conf. Comput. Commun. Convergence Technol. (I2CT), 1–8 (2023). https://doi.org/10.1109/MetaCom57706.2023.00079

[14] G. Tripathi, F. Siddiqui, M. A. Alam, M. A. Ahad, M. M. Akhtar, G. Casalino, BAuth-ZKP—A blockchain-based multi-factor authentication mechanism for securing smart cities. Sensors **23**(5), 2757 (2023). https://doi.org/10.3390/s23052757

[15] Y. Zhang, B. Li, J. Wu, B. Liu, R. Chen, J. Chang, Efficient and privacy-preserving blockchain-based multifactor device authentication protocol for cross-domain Industrial Internet of Things. IEEE Internet Things J. **9**(22), 22501–22515 (2022). https://doi.org/10.1109/JIOT.2022.3176192