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)

!394-2975 | 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.2025.1203070

Secure Identity and Key Management in Edge Computing Via Multi-Layer Blockchain

A. Lakshmipathi Rao[1], T. Sushma[2], S. Priyadarshini [3], V. Lakshmi Manasa[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[2-4]

ABSTRACT: In today's rapidly evolving digital landscape, where billions of IoT devices are interconnected, ensuring secure communication through robust identity authentication and key agreement mechanisms has become imperative. Particularly in edge computing environments, where IoT devices operate across multiple, heterogeneous security domains and frequently engage in cross-domain interactions, traditional authentication schemes face substantial challenges. These conventional methods, largely dependent on Public Key Infrastructure (PKI), often present centralized points of failure and lack the scalability and resilience required for distributed edge architectures.To address these limitations, this project proposes an advanced identity authentication and key agreement framework leveraging blockchain technology. Specifically, we design a multi-layer blockchain-based authentication architecture tailored for IoT ecosystems. This architecture enables secure, decentralized management of digital identities and supports seamless cross-domain authentication. By recording the hash values of digital certificates on the blockchain and integrating dynamic accumulator technology, the system significantly enhances the reliability, traceability, and efficiency of certificate verification processes.The proposed solution not only eliminates the risks associated with centralized authentication but also ensures scalability and adaptability in diverse network environments. Security analysis confirms the robustness of the model against common attacks, while experimental evaluations demonstrate its efficiency in real-world scenarios. Overall, the integration of multi- layer blockchain and cryptographic techniques presents a practical and secure approach to identity authentication and key agreement in edge-enabled IoT infrastructures

I.INTRODUCTION

This paper is primarily based on the distributed architecture of edge computing networks. In order to address the cross-domain requests from IoT devices in different security domains, we have designed a multi-layer blockchain authentication architecture and proposed a protocol scheme for identity authentication and key agreement for both single-domain and cross-domain terminal devices based on the multi-layer blockchain.The hash value of the digital certificate is stored on the blockchain, which improves the reliability of the digital certificate. It also simplifies the digital certificate reliability verification process, reduces the number of signature verification and improves authentication efficiency. To solve the problem of inefficient on-chain data queries due to the increased size of the blockchain, the authentication process incorporates dynamic accumulator technology to improve the efficiency of the authentication process certificate verification. The protocol designed in this paper was analyzed for security and performance. The results indicate that the protocol meets security requirements, as demonstrated by formal security analysis tools and proof of protocol security under the ROR model. Comparing its performance with similar cross-domain authentication protocols shows that this protocol exhibits good computational performance.

II. LITERATURE SURVEY

Title: Digital twin-based drone-assisted secure data aggregation scheme with federated learning inartificial intelligence of things.
Year: 2023**Author:** A. Islam and S. Y. Shin.
Description: The Artificial Intelligence of Things (AIoT) is transforming everyday life by combining the power of artificial intelligence (AI) with the Internet of Things (IoT), promising greater efficiency and smarter automation. However, putting this vision into practice isn't without its challenges. Limited resources—especially in terms of computational

!394-2975 | 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.2025.1203070

power—make it difficult to effectively implement advanced technologies like AI within IoT systems. In addition, growing concerns about cyber threats and data privacy pose significant obstacles to widespread adoption. These issues are further compounded by poor or inconsistent network connectivity, which can limit the performance of IoT systems.

To address these challenges, this article introduces a digital twin-based data aggregation framework. In this setup, data are collected using federated learning via drones, and then securely stored on a blockchain network. To protect privacy before sharing the data, differential privacy techniques are applied.

The framework also includes a multi-role training scheme and a dual-layer model verification process that uses a Hampel filter along with performance evaluation. To ensure secure and reliable operations, an authentication mechanism is implemented by combining a cuckoo filter with timeframe validation.

To test the practicality of the proposed system, a case study was conducted using real hardware to build a functioning experimental environment. Multiple tests were carried out in this setup, and the results demonstrated the feasibility and effectiveness of the approach.

The Internet of Things (IoT) is becoming an essential part of modern life, thanks to its ability to sense and interact with the environment in intelligent ways. However, the sheer volume of sensitive data generated—such as health-related information—raises serious privacy concerns. In this context, AIoT offers a promising solution by enhancing the capabilities of IoT systems through AI integration. Yet, limitations in processing power and vulnerability to cyber attacks (such as man- in-the-middle threats), along with network constraints, still present major hurdles—especially when aggregating data from IoT devices.

Title: PUF-based authentication and key agreement protocols for IoT, WSNs, and smart grids: A comprehensive survey.
Year: 2022
Author: P. Mall, R. Amin, A. K. Das, M. T. Leung, and K. R. Choo.
Description: A Physically Unclonable Function (PUF) is a hardware-based security feature built into sensors, providing a unique and unreplicable key derived from a device's physical characteristics. It serves as a reliable trust anchor for resource- constrained devices. Authentication and Key Agreement (AKA) protocols enable secure communication by allowing devices to authenticate each other and exchange session keys. Though widely used in secure transactions, these protocols remain vulnerable to various cyber threats.
This article:
Reviews AKA protocols, PUFs, and PUF-based AKA systems.
Analyzes their use in IoT, wireless sensor networks, and smart grids.
Highlights challenges, security risks, and mitigation strategies.
Presents a performance and security comparison across the three domains.
In sensor networks, each sensor node can gather, process, and share data. It typically includes a controller, transceiver, sensor, memory, and power source. Microcontrollers are commonly used due to their low cost and flexibility.

Title: Toward cross-domain dynamic accumulator authentication based on blockchain in Internet of Things.
Year: 2022
Author: L. Wang, Y. Tian, and D. Zhang.
Description: Authentication remains a major challenge in Internet of Things (IoT) applications, especially across different management domains. This article addresses the issue by introducing relationship authentication among smart devices as a solution to cross-domain verification.

The approach starts by modeling device authentication relationships as a general undirected graph. The authentication problem is then reframed as a signature transitivity problem, using accumulator-based cryptography and standard digital signatures. This allows devices to verify authentication across domains without knowing each other's administrative background.

To ensure continuous availability and reduce the burden on a central authority, the scheme integrates blockchain technology, enabling a 24/7 trusted third party. Experimental results show that the proposed method, CroDA, effectively handles real- world authentication challenges in IoT.

As IoT expands across sectors like healthcare, smart grids, traffic systems, and smart homes, different sets of devices form their own IoT domains. These domains are interconnected using communication technologies to enable resource sharing and service delivery regardless of location.

!394-2975 | 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.2025.1203070

Title: A blockchain based mutual authentication scheme for collaborative edge computing.
Year: 2022
Author: G. Cheng, Y. Chen, S. Deng, H. Gao, and J. Yin.
Description: With the rising demand for delay-sensitive and mission-critical applications, edge computing has emerged as a key solution to reduce the load on traditional cloud-based IoT systems. By placing edge servers closer to end-users, Collaborative Edge Computing (CEC) enables real-time computation and communication, improving service latency and bandwidth.
However, this architecture introduces new risks: compromised edge servers and fake IoT devices can threaten system security. To address this, a secure and efficient mutual authentication scheme is essential. While several methods have been proposed, many fall short due to a lack of decentralization, anonymity, and mobility support.
To overcome these limitations, we propose a blockchain-based mutual authentication scheme that combines certificateless cryptography, elliptic curve cryptography, and pseudonym-based methods. Our solution supports both intra-edge and inter-edge authentication and includes detailed procedures for key generation and session key negotiation.
Extensive testing and security analysis demonstrate the scheme's feasibility. Moreover, by reducing communication distance and offloading heavy tasks to edge servers, this approach lowers latency, balances network traffic, and extends the lifespan of IoT devices.

Title: Blockchain on security and forensics management in edge computing for IoT: A comprehensive survey.
Year: 2022
Author: Z. Liao, X. Pang, J. Zhang, B. Xiong, and J. Wang.
Description:
Security and forensics are essential for managing large-scale networks like the Internet of Things (IoT). To meet the demands of low-latency, high-speed communication, Mobile Edge Computing (MEC) brings computing power closer to IoT devices, reducing reliance on distant cloud servers.
MEC systems involve three key components: the devices, the data they generate, and the digital evidence created through data interactions. These elements are widely distributed, making traditional centralized security methods insufficient.
Blockchain—as a decentralized, tamper-proof, and traceable ledger—offers a promising solution. Its ability to ensure data integrity, confidentiality, and anonymity has sparked growing interest in combining blockchain with MEC to enhance device security, data protection, and digital forensics in IoT environments.
This survey explores the integration of blockchain in MEC-IoT systems, focusing on current technologies and strategies to address security and forensic challenges. It also highlights open issues and future research directions in this evolving field.

Title: An effective privacy-preserving blockchain-assisted security protocol for cloud-based digital twin environment.
Year: 2023
Author: G. Thakur, P. Kumar, Deepika, S. Jangirala, A. K. Das, and Y. Park.
Description:
Digital Twin (DT) technology is gaining widespread attention for its applications in industries like manufacturing, aerospace, and healthcare. DT involves creating a virtual replica of a physical object to enable real-time monitoring, simulation, and predictive maintenance. However, these advantages come with significant security and privacy risks during deployment.
To address this, various authentication protocols have been proposed. This article reviews a recent two-factor authentication scheme using blockchain for DT environments, which unfortunately falls short in resisting key attacks like offline password guessing, smart card theft, and impersonation. To overcome these limitations, we propose a three-factor privacy-preserving authentication scheme, which offers stronger protection.
Our proposed method is validated through informal security analysis, formal verification using BAN logic, and the Real-or-Random (ROR) model. Comparative studies show that our scheme offers better security with lower computational costs and similar communication overhead compared to existing approaches.
Cloud computing plays a central role in DT systems by hosting services and enabling data sharing between physical assets and users. However, ensuring secure and trustworthy data sharing is critical. If simulation or real-time data is intercepted, it can lead to severe privacy breaches.

To securely deploy DT environments, the following must be ensured:

!394-2975 | 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.2025.1203070

1. A secure medium for efficient data transmission.
2. Mechanisms for data integrity verification.
3. Fulfillment of security requirements like anonymity, untraceability, and confidentiality.

Our solution leverages blockchain to enhance security. It stores data hash values on the blockchain, allowing users to verify data integrity via Merkle hash trees. All data sharing transactions are also logged on the blockchain for transparency and traceability.

Title: Design of secure mutual authentication scheme for metaverse environments using blockchain.
Year: 2023
Author: J. Ryu, S. Son, J. Lee, Y. Park, and Y. Park.
Description:
During the COVID-19 pandemic, the use of remote platforms for activities like online education and virtual meetings significantly increased. However, traditional online environments—based on simple video and audio streaming—lacked the ability to convey physical interactions and real-world experiences, such as cultural or economic activities.
To bridge this gap, metaverse platforms like Roblox, Minecraft, and Fortnite have gained popularity, offering immersive, 3D virtual environments using avatars. Despite their benefits, these platforms are vulnerable to security threats, as communications occur over public channels and sensitive user data (e.g., identity, passwords, biometrics) are stored by the platform servers.
This paper presents a blockchain-based system model designed to secure communications and manage user identity data transparently in the metaverse. We propose a mutual authentication scheme that uses biometric data and Elliptic Curve Cryptography (ECC) to ensure secure interactions between users, servers, and avatars.
To verify the security of our proposed scheme, we conduct several analyses:

- Informal security review
- BAN logic
- Real-or-Random (ROR) model
- AVISPA tool (Automated protocol validation)

We also compare the computational and communication costs and security capabilities of our scheme against existing ones. The results show that our approach offers lower overhead and broader security coverage, making it a more effective solution for secure metaverse environments.

III. EXISTING SYSTEM

- At present, traditional identity authentication methods are mostly based on Public Key Infrastructure (PKI) implementation, which belongs to centralized authentication.
- The centralized authentication process requires the involvement of a trusted third party and is prone to single point of failure issues.
- The security of this type of authentication relies on the stability of the Certificate Authority (CA).

EXISTING SYSTEM DISADVANTAGES

- The edge server domain is involved in maintaining less security.
- Less the reliability and authentication efficiency of the digital certificate.
- Data sharing in different security domains, identity authentication faces a series of challenges and security issues

IV. PROPOSED SYSTEM

This paper is primarily based on the distributed architecture of edge computing networks.In order to address the cross-domain requests from IoT devices in different security domains, we have designed a multi-layer blockchain authentication architecture and proposed a protocol scheme for identity authentication and key agreement for both single-domain and cross-domain terminal devices based on the multi-layer blockchain.In this paper was analyzed for security and performance. The results indicate that the protocol meets security requirements, as demonstrated by formal security analysis tools and proof of protocol security.

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

!394-2975 | 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.2025.1203070

PROPOSED SYSTEM ADVANTAGES

The edge server within each more security domain is involved in maintaining the local blockchain.
Enhance the reliability and authentication efficiency of the digital certificate.
Our scheme can achieve efficient and secure authentication and key agreement.

V. SYSTEM ARCHITECTURE

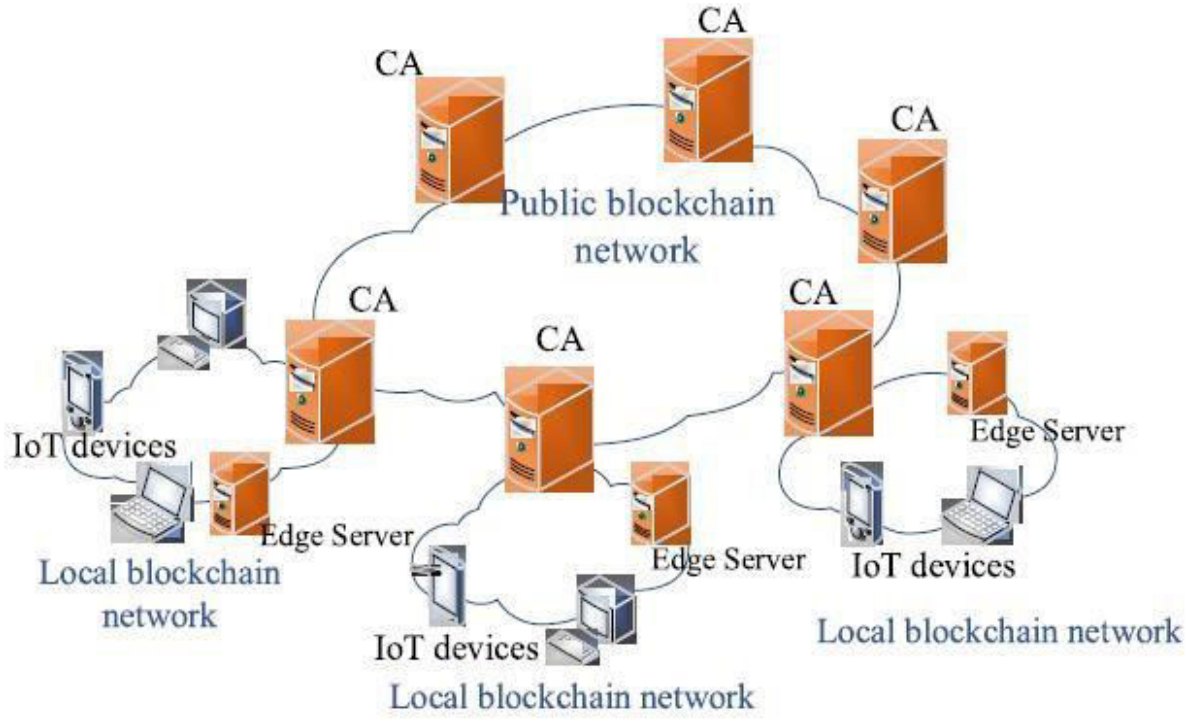

Fig:1

The system architecture of multi-layer blockchain designed in this paper is composed of local blockchain network and public blockchain network. Terminal devices, edge server, and local certificate authority CA belonging to the same security domain together form the local blockchain network. Certificate authorities in different security domains form a public blockchain network. When terminal devices belonging to different security domains need to authenticate communication, they can use the public blockchain network as a communication bridge. The local blockchain and public blockchain are built based on the prototype of the alliance chain, and only approved nodes are allowed to join the blockchain network.

VI. METHODOLOGIES

Modules Name:
This project having the following 5 modules:

- **User Interface Design**
- **Cloud Server**
- **Certificate Authority (CA) or Network Authority**
- **Data Owner**
- **Data User**
- **Key Agreement Protocol Module**
- **Multilayer Blockchain**

1. User Interface Design

!394-2975 | 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.2025.1203070

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. Logging in is usually used to enter a specific page. It will search the query and display the query.

2.The Data User:

Each data user has a set of attributes register users with unique identities using cryptographic methods. Generate digital identities or certificates based on public-private key pairs. Store and manage user credentials securely on the blockchain.DU logins onto the system and sends, an authorization request to CA. The authorization request includes attribute keys (SK) which DU already has. TA accepts the authorization request and checks the request and a generate attribute keys (SK) for DU. DU sends a request for data to the cloud. Cloud receives the request and checks if the DU meets the accessrequirement. DU receives the ciphertext, which includes ciphertext of data files and ciphertext of the symmetric ey. DU decrypt the ciphertext of the symmetric key with the assistance of DSP. DU uses the symmetric key to decrypt the ciphertext of data files.

3. Cloud Server:

The cloud process authentication and key agreement tasks at the edge nodes to reduce latency. Enable secure storage and real- time processing of user data near the source. Offload computational tasks from the blockchain network to edge nodes.

4. Certificate Authority (CA)

Certificate authorities in different security domains form a public blockchain network. When terminal devices belonging to different security domains need to authenticate communication, they can use the public blockchain network as a communication bridge. The local blockchain and public blockchain are built based on the prototype of the alliance chain, and only approved nodes are allowed to join the blockchain network.

The method of certificate verification is carried out by comparing the certificate hash submitted by the cross-domain user with the certificate hash stored on the blockchain. This approach increases the query time when searching on the blockchain, as it necessitates traversing the entire blockchain. In this paper, however, we employ a dynamic accumulator in the authentication process to reduce the certificate query time complexity.

5. Key Agreement Protocol Module:

Establish secure session keys between users and devices via blockchain-based negotiation. Enable lightweight, energy-efficient key exchange suitable for edge environments. Ensure resistance to attacks such as man-in-the-middle and replay attacks. Authenticate user identities using blockchain-validated credentials. Ensure mutual authentication between devices, users, and edge nodes. Other secure methods to protect user privacy

6. Data Owner:

When the data owner (DO) registers on CA, CA runs the algorithm Setup() to generate a public key PK and a master key MK. PK is sent to DO while MK is kept on CA itself. DO defines its own attribute set and assigns attributes to its contacts. All these information will be sent to CA and the cloud. CA and the cloud receive the information and store it. DO uploads data to the mobile cloud and share it with friends. DO determines the access control policies. DO sends data to the cloud. Since the cloud is not credible, data has to be encrypted before it is uploaded. The DO defines access control policy in the form of access control tree on data files to assign which attributes a DU should obtain if he wants to access a certain data file.

7. Multi-Layer Blockchain Provides

Multi-layer blockchain designed in this paper is composed of local blockchain network and public blockchain network.Multi-layer blockchain provides distributed authentication with the help of blockchain technology.Different security domains correspond to a local blockchain to establish a local collaborative trust network. The data processed by a single device is distributed to multiple edge servers for collaborative processing, which ensures the consistency and security of decentralized IoT systems. The multi-tier blockchain is composed of a public blockchain and a local blockchain. Both

!394-2975 | 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.2025.1203070

public or local blockchains are based on federated chain composition. External nodes can join only after getting approval from the audit to improve the security of the system architecture.

VII. ALGORITHM USED

EXISTING TECHNIQUE: -

Public Key Infrastructure

A blockchain based BB-PKI to manage certificates. To avoid single point of failure, multiple CAs issue certificates and record certificate transactions on the blockchain through smart contracts .A decentralized authentication model using identity- based own authentication algorithm instead of PKI. The model is based on blockchain combined with smart contracts and threshold ciphers and has good flexibility.

PROPOSED TECHNIQUE USED: -

Identity Authentication and Key Agreement in Cross-Domain

The cross-domain authentication and key agreement process in this section will add new information on the basis of local digital certificates to generate cross-domain certificates. The cross-domain authentication process will re-issue cross-domain certificates as explained below. If the certificate obtained on the local blockchain continues to be used in the cross-domain authentication process. Cross-domain authentication using certificates on the local blockchain can make cross-domain access lesssecure.

VIII.EXPERIMENTAL RESULTS

Fig 1: Home Page

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

!394-2975 | 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.2025.1203070

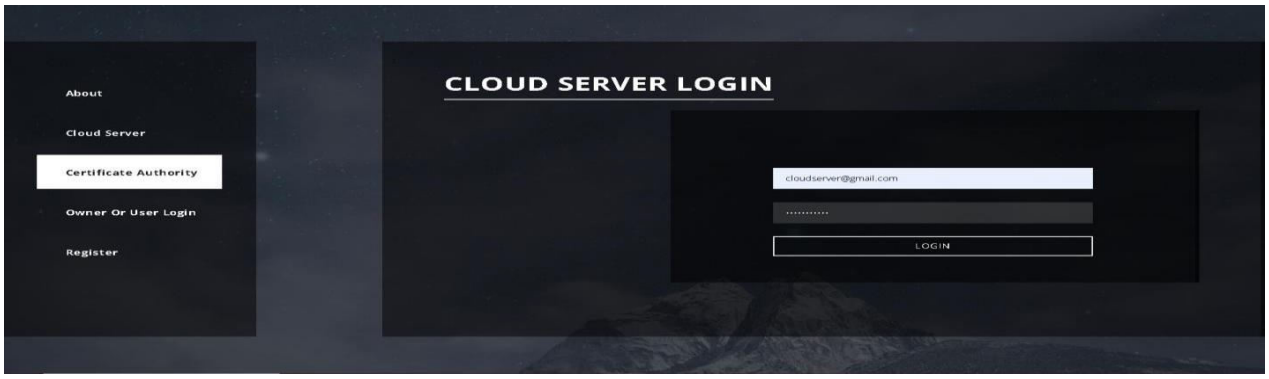

Fig 2: Cloud Server Login Page

Fig 3: Certificate Authority Login Page

Fig 4: Data owner or User Registration Page

Fig 5: Data Owner or User Login Page

!394-2975 | 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.2025.1203070

IX. CONCLUSION

In the edge-computing environment, this scheme proposes a cross-domain authentication and key agreement protocol based on a multi-layer blockchain. Cross-domain authentication of IoT devices with different security domains is achieved. A multi-layer blockchain architecture is designed, consisting of a local blockchain and a public blockchain. Dynamic accumulator is introduced to solve the problem of inefficient certificate lookups. Next, we conducted performance and security analysis, and the results showed that the protocol is well feasible and efficient, and more adaptable with low performance devices.

X. FUTURE ENHANCEMENT

Further in-depth research on the underlying blockchain technology is needed in the future to make blockchain technology an important tool for identity authentication and key agreement.

REFERENCES

1. The Mobile Economy 2020, London, U.K., 2019, [online] Available: https://www.gsma.com/.
2. A.Islam and S. Y. Shin, "A digital twin-based drone-assisted secure data aggregation scheme with federated learning in artificial intelligence of things", IEEE Netw., vol. 37, no. 2, pp. 278-285, Mar. 2023.
3. P. Mall, R. Amin, A. K. Das, M. T. Leung and K. R. Choo, "PUF-based authentication and key agreement protocols for IoT WSNs and smart grids: A comprehensive survey", IEEE Internet Things J., vol. 9, no. 11, pp. 8205-8228, Jun. 2022.
4. P. Kumar, R. Kumar, G. Srivastava, G. P. Gupta, R. Tripathi, T. R. Gadekallu, et al., "PPSF: A privacy-preserving and secure framework using blockchain-based machine-learning for IoT-driven smart cities", IEEE Trans. Netw. Sci. Eng., vol. 8, no. 3, pp. 2326-2341, Jul. 2021.
5. Y. Lu, X. Huang, K. Zhang, S. Maharjan and Y. Zhang, "Blockchain empowered asynchronous federated learning for secure data sharing in Internet of Vehicles", IEEE Trans. Veh. Technol., vol. 69, no. 4, pp. 4298-4311, Apr. 2020.
6. X. Xiang, M. Wang and W. Fan, "A permissioned blockchain-based identity management and user authentication scheme for E-health systems", IEEE Access, vol. 8, pp. 171771-171783, 2020.
7. S. He, Z. Li, J. Wang and N. N. Xiong, "Intelligent detection for key performance indicators in industrial-based cyber-physical systems", IEEE Trans. Ind. Informat., vol. 17, no. 8, pp. 5799-5809, Aug. 2021.
8. W. Shi, J. Cao, Q. Zhang, Y. Li and L. Xu, "Edge computing: Vision and challenges", IEEE Internet Things J., vol. 3, no. 5, pp. 637-646, Oct. 2016.
9. J. B. Xue and Z. M. Bai, "Security and efficient authentication scheme for mobile edge computing", J. Beijing Univ. Posts Telecommun., vol. 44, no. 1, pp. 110-116, Jan. 2021.
10. O. Salman, S. Abdallah, I. H. Elhajj, A. Chehab and A. Kayssi, "Identity-based authentication scheme for the Internet of Things", Proc. IEEE Symp. Comput. Commun. (ISCC), pp. 1109-1111, Jun. 2016.
11. K. Xue, P. He, X. Zhang, Q. Xia, D. S. L. Wei, H. Yue, et al., "A secure efficient and accountable edge-based access control framework for information centric networks", IEEE/ACM Trans. Netw., vol. 27, no. 3, pp. 1220-1233, Jun. 2019.
12. P. Black and R. Layton, "Be careful who you trust: Issues with the public key infrastructure", Proc. 5th Cybercrime Trustworthy Comput. Conf., pp. 12-21, Nov. 2014.
13. J. Ni, K. Zhang, X. Lin and X. Shen, "Securing fog computing for Internet of Things applications: Challenges and solutions", IEEE Commun. Surveys Tuts., vol. 20, no. 1, pp. 601-628, 1st Quart. 2018.
14. T. Salman, M. Zolanvari, A. Erbad, R. Jain and M. Samaka, "Security services using blockchains: A state of the art survey", IEEE Commun. Surveys Tuts., vol. 21, no. 1, pp. 858-880, 1st Quart. 2019.
15. B. Cao, Y. Li, L. Zhang, L. Zhang, S. Mumtaz, Z. Zhou, et al., "When Internet of Things meets blockchain: Challenges in distributed consensus", IEEE Netw., vol. 33, no. 6, pp. 133-139, Nov. 2019.
16. S. Matsumoto and R. M. Reischuk, "IKP: Turning a PKI around with decentralized automated incentives", Proc. IEEE Symp. Secur. Privacy (SP), pp. 410-426, May 2017.
17. A. Garba, Q. Hu, Z. Chen and M. R. Asghar, "BB-PKI: Blockchain-based public key infrastructure certificate management", Proc. IEEE 22nd Int. Conf. High Perform. Comput. Commun.; IEEE 18th Int. Conf. Smart City; IEEE 6th Int. Conf. Data Sci. Syst. (HPCC/SmartCity/DSS), pp. 824-829, Dec. 2020.

!394-2975 | 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.2025.1203070

18. Garba, Z. Chen, Z. Guan and G. Srivastava, "LightLedger: A novel blockchain-based domain certificate authentication and validation scheme", IEEE Trans. Netw. Sci. Eng., vol. 8, no. 2, pp. 1698-1710, Apr. 2021.
19. P. Gu and L. Chen, "An efficient blockchain-based cross-domain authentication and secure certificate revocation scheme", Proc. IEEE 6th Int. Conf. Comput. Commun. (ICCC), pp. 1776-1782, Dec. 2020.
20. W. Wang, N. Hu and X. Liu, "BlockCAM: A blockchain-based cross-domain authentication model", Proc. IEEE 3rd Int. Conf. Data Sci. Cyberspace (DSC), pp. 896-901, Jun. 2018.
21. Yuan, W. Zhang and X. Wang, "EIMAKP: Heterogeneous cross-domain authenticated key agreement protocols in the EIM system", Arabian J. Sci. Eng., vol. 42, no. 8, pp. 3275-3287, Aug. 2017.
22. He, S. Chan and M. Guizani, "An accountable privacy-preserving and efficient authentication framework for wireless access networks", IEEE Trans. Veh. Technol., vol. 65, no. 3, pp. 1605-1614, Mar. 2016.
23. He, J. Bu, S. Chan, C. Chen and M. Yin, "Privacy-preserving universal authentication protocol for wireless communications", IEEE Trans. Wireless Commun., vol. 10, no. 2, pp. 431-436, Feb. 2011.
24. L. Wang, Y. Tian and D. Zhang, "Toward cross-domain dynamic accumulator authentication based on blockchain in Internet of Things", IEEE Trans. Ind. Informat., vol. 18, no. 4, pp. 2858-2867, Apr. 2022.
25. M. Wang, L. Rui, Y. Yang, Z. Gao and X. Chen, "A blockchain-based multi-CA cross-domain authentication scheme in decentralized autonomous network", IEEE Trans. Netw. Service Manage., vol. 19, no. 3, pp. 2664-2676, Sep. 2022.
26. X. Jia, N. Hu, S. Su, S. Yin, Y. Zhao, X. Cheng, et al., "IRBA: An identity-based cross-domain authentication scheme for the Internet of Things", Electronics, vol. 9, no. 4, pp. 634, Apr. 2020.
27. S. Guo, F. Wang, N. Zhang, F. Qi and X. Qiu, "Master-slave chain based trusted cross-domain authentication mechanism in IoT", J. Netw. Comput. Appl., vol. 172, Dec. 2020.
28. G. Cheng, Y. Chen, S. Deng, H. Gao and J. Yin, "A blockchain-based mutual authentication scheme for collaborative edge computing", IEEE Trans. Computat. Social Syst., vol. 9, no. 1, pp. 146-158, Feb. 2022.
29. S. Showkat Moni and D. Manivannan, "A lightweight privacy-preserving V2I mutual authentication scheme using cuckoo filter in VANETs", Proc. IEEE 19th Annu. Consum. Commun. Netw. Conf. (CCNC), pp. 815-820, Jan. 2022.
30. J. Qi, "Research on the application of accumulator in blockchain", 2020.
31. M. X. Miao, P. R. Wu and Y. L. Wang, "Research progress and application of password accumulator", J. Xidian Univ., vol. 49, no. 1, pp. 79-91, Sep. 2022.
32. J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang and W. Zhao, "A survey on Internet of Things: Architecture enabling technologies security and privacy and applications", IEEE Internet Things J., vol. 4, no. 5, pp. 1125-1142, Oct. 2017.
33. V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal and B. Sikdar, "A survey on IoT security: Application areas security threats and solution architectures", IEEE Access, vol. 7, pp. 82721-82743, 2019.
34. Z. Liao, X. Pang, J. Zhang, B. Xiong and J. Wang, "Blockchain on security and forensics management in edge computing for IoT: A comprehensive survey", IEEE Trans. Netw. Service Manage., vol. 19, no. 2, pp. 1159-1175, Jun. 2022.
35. H. K. Jiang et al., "Improved certificateless proxy blind signature scheme with forward security", Comput. Sci., vol. 48, no. 6A, pp. 529-532, Jun. 2021.
36. N. Kahya, N. Ghoualmi and P. Lafourcade, "Formal analysis of PKM using scyther tool", Proc. Int. Conf. Inf. Technol. e-Services, pp. 1-6, Mar. 2012.
37. G. Thakur, P. Kumar, Deepika, S. Jangirala, A. K. Das and Y. Park, "An effective privacy-preserving blockchain- assisted security protocol for cloud-based digital twin environment", IEEE Access, vol. 11, pp. 26877-26892, 2023.
38. J. Ryu, S. Son, J. Lee, Y. Park and Y. Park, "Design of secure mutual authentication scheme for metaverse environments using blockchain", IEEE Access, vol. 10, pp. 98944-98958, 2022.
39. M. Bellare, R. Canetti and H. Krawczyk, "A modular approach to the design and analysis of authentication and key-exchange protocols", Proc. 30th Annu. ACM Symp. Theory Comput. (STOC), pp. 419-428, May 1998.FISCO-BCOS, Oct. 2020, [online] Available: https://wwwfisco-bcos.org.

International Journal of Advanced Research in Education and Technology

ISSN: 2394-2975 Impact Factor: 8.152

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