International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research Paper

A NEW IDENTITY AUTHENTICATION AND KEY AGREEMENT PROTOCOL BASED ON MULTI-LAYER BLOCKCHAIN IN EDGE COMPUTING

NAVEEN REDDY NEMILI [1], KAMBHAMPATI BHANU PRAKASH [2], JEEDIPALLY SHARANYA [3], KAKARA RAMBABU [4], CHINNAM NARESH [5]

[1]Assistant Professor, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

[2, 3, 4, 5] B.Tech, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

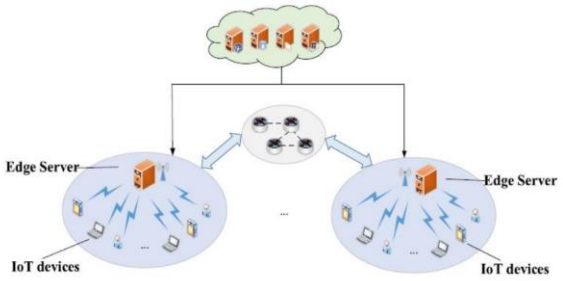
ABSTRACT— In today's interconnected world, identity authentication and key agreement are important links in the secure communication process of IoT terminal devices. In the edge computing environment, with the frequent cross-domain authentication and data sharing of IoT devices in different security domains, identity authentication faces a series of challenges and security issues. Most of the traditional identity authentication methods are based on public key infrastructure, which is prone to single point of failure and is not applicable to the distributed architecture of edge computing. In this article, we apply blockchain technology to the identity authentication and key agreement process of IoT terminal devices. In order to meet cross-domain requests from terminal devices in different security domains, a multi-layer blockchain authentication architecture is designed. The hash value of the digital certificate is stored on the blockchain and combined with dynamic accumulator technology to enhance the reliability and authentication efficiency of the digital certificate. Security analysis and experimental results demonstrate that our scheme can achieve efficient and secure authentication and key agreement.

Index Terms – Identity Authentication, Key Agreement, Multi-Layer Blockchain, Edge

Computing, Mutual Authentication, Secure Communication, Cryptography, IoT Security, Distributed Ledger Technology, Cybersecurity.

I. INTRODUCTION

Nowadays, we are witnessing the rapid proliferation of intelligent devices in the digital age, ushering in an era of interconnected everything. The IoT exhibits characteristics such as multi-source heterogeneity and openness, but it also confronts challenges related to cyber threats and privacy. This makes the protection of the identity information of IoT devices of great significance to individuals, families, society and even national security. The applications of the Internet of Things span various domains, including the smart grid smart cities intelligent transportation healthcare and the industrial Internet of Things. With the advancement of the Internet, a large number of terminal devices are being connected to the network. Traditional cloud centers suffer from data processing delays, resulting in a heavy burden on cloud center authentication. The traditional cloud-computing environment falls short of meeting the growing demand. The introduction of edge computing aims to alleviate the computing pressure on the cloud center by diverting data flow. Edge servers are deployed to take over certain functions of the cloud center and handle the computing and storage tasks of devices in close proximity to the terminals. 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). The authentication process uses digital certificates issued by CAs to authenticate identities. Once a CA is attacked, it will result in identity authentication being unable to proceed.



Digital certificate verification in the authentication process needs to be completed by public key encryption and digital signature. This leads to complication of certificate verification process, longer

verification times and verification time. There are multiple security domains for identity authentication in the edge-computing environment and the authentication hierarchy is complex. Massive terminal devices need to cross-domain authentication under different security domains to request frequent data access. In order to ensure the consistency and security of the distributed Internet of Things system, we provide a distributed authentication scheme using blockchain technology. Blockchain itself is a distributed network architecture. The binding energy of blockchain and edge computing can well solve the security problems in identity authentication. Due to its decentralized, tamper proof, open and transparent characteristics, blockchain technology can solve the single point of failure problem of public key infrastructure-based authentication. Therefore, the use of blockchain technology can establish communication channels for IoT devices in different security domains.

II. RELATED WORK

A. Digital twin-based drone-assisted secure data aggregation scheme with federated learning in artificial intelligence of things

Artificial intelligence of things (AIoT) has brought new promises of efficiency in our daily lives by integrating AI with the IoT. However, owing to limited resources (e.g., computational power), it is difficult to implement modern technology (e.g., AI) and improve its performance (i.e., the IoT). Moreover, cyber threats and privacy challenges can hinder the success of the IoT. This situation is aggravated by network scarcity (i.e., limited network connectivity). This article presents a digital twin-based data aggregation scheme in which data are collected using federated learning by operating a drone and stored securely in the blockchain. Before data sharing, differential privacy is realized to enhance privacy. A multirole training scheme is proposed, along with a duplex model verification architecture using a Hampel filter and performance check. To validate the specifications, an authentication scheme was implemented by combining a cuckoo filter and timeframe check. A case study to construct an experimental environment using real hardware is discussed. Different experiments were conducted in this environment and the feasibility of the proposed scheme was validated from the outcomes. The internet of things (IoT) is becoming important and ubiquitous in our daily lives owing to its

smart sensing and actuation capabilities. Given that the IoT can produce a large amount of sensitive information (e.g., health data), new privacy concerns are raising as a result of the potential sharing of these data. A new promising paradigm, called artificial intelligence (AI) of things (AIoT), has emerged in which AI is integrated with the IoT to increase the efficiency of IoT operations. However, owing to limited computational capabilities, the difficulty of integrating the IoT with other technologies (e.g., AI) for performance enhancement has increased. In addition, the IoT encompasses other cyberthreats (e.g., man-in-the- middle attacks) and network scarcity can degrade the performance during data aggregation from IoT devices.

B. PUF-based authentication and key agreement protocols for IoT, WSNs, and smart grids: A comprehensive survey.

Physically unclonable function (PUF) is a physical unit fabricated inside a sensor and generally considered as an assurance anchor of resource inhibited device. Essentially, the function is based on the cryptographic approach, where a key is created and utilized such that it cannot be cloned. More specifically, it is an arbitrary function, which maps inherent properties of the hardware devices to a unique bit stream of information. Authentication and key agreement (AKA) protocols are widely used in electronic commerce, electronic stock trading, and many secured business transaction platforms, because they allow the communicating devices to mutually authenticate, each other while exchanging authenticated session key (or secret key) that can be used subsequently to establish a secured communication channel. Yet, these protocols are also vulnerable to a broad range of security outbreaks. In light of these notions and practical applications, this article is intended to: 1) provide an overview of AKA protocols, PUF plus the combined PUF-based AKA; 2) systematically and taxonomically examine and discuss with pros and cons of AKA applications to the fast growing areas of Internet of Things, wireless sensor networks, and smart grids based on a meticulous survey of the existing literature; 3) summarize the challenges to deployment and potential security risks of the underlying technologies and possible remedies or mitigation strategies; and 4) to conduct and report a comparative performance and security analysis with respect to the three focused areas. A node in the sensor network, commonly referred as a sensor node, has the capacities to perform assembling and

processing of sensitive data as well as to communicate with other adjoining nodes in the network. Typically, a sensor node consists of five major components: 1) a controller; 2) a transceiver; 3) a sensor; 4) an external memory; and 5) a power source. To be specific, a controller in a sensor node completes certain tasks, processes data, and controls the node's component functionality. Microcontroller is a type of controller widely used in sensor nodes because of its inexpensiveness and elasticity in connecting to other devices.

C. Toward cross-domain dynamic accumulator authentication based on blockchain in Internet of Things

The authentication problem is one of the most significant challenges in the applications of Internet of Things (IoT), and the relationship authentication among smart devices is an effective solution to tackle cross-domain issue. In this article, we first abstract a general undirected graph from the authentication relationship among the smart devices in IoT. Then, we formulate the authentication problem into a signature transitivity problem by incorporating accumulator knowledge and a standard digital signature scheme. As a consequence, the legality of authentication is well-verified by computing the signature and witness of the related edges without worrying about whether the devices belong to the same administrative domain or not. Finally, the efficiency and online time of authority are solved by exploring the blockchain technology, which also leads to the assurance of an online 24-hour third party. The results of analysis and comparison show that the proposed scheme CroDA can well address the practical authentication issue. The omnipresence of the idea behind IoT and its variety services, the evolution of many areas gradually have equipped corresponding infrastructure in order to provide a wide range of services regardless of their location, such as health care, smart grid, traffic managements, and smart homes. And these IoT devices in aforementioned for environment have their own management domains. Thereby, these IoT devices in the same management domain compose an IoT domain, and the different IoT domains are connected by communication technology to share resources.

III. PROPOSED METHODOLOGY

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.

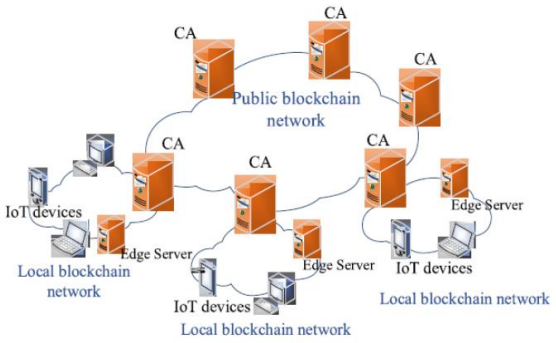
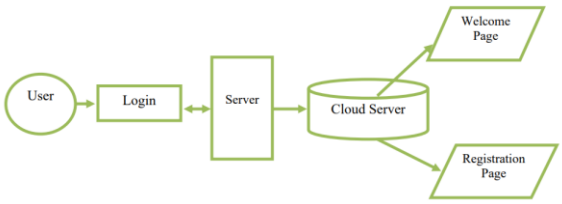


Fig. 1: System Overview

1. User Interface Design

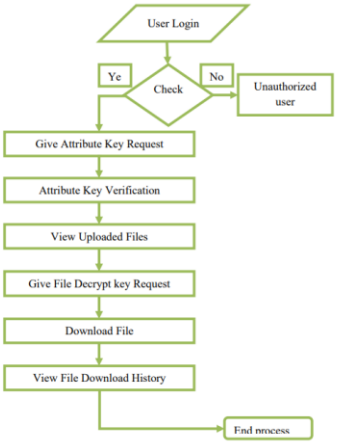
To connect with server user must give their username and password then only they can able to connect the server. If the user already exits directly can login into the server else, user must register their details such as username, password, Email id, City and Country into the server. Database will create 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. Data User:

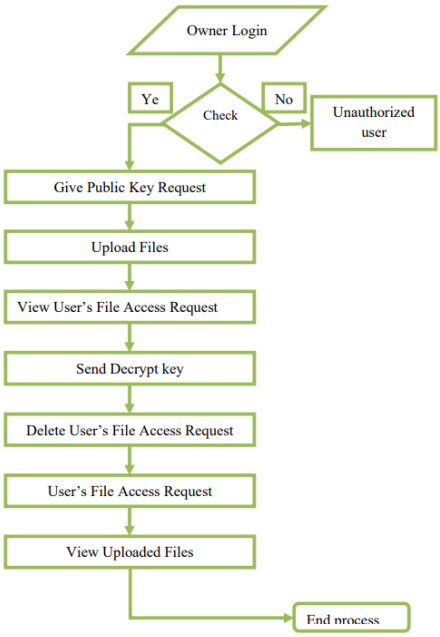
Each data user has a set of attributes register users with unique identities using cryptographic methods. Generate digital identities or certificates based on public-private key pairs. Store and manage user credentials securely on the blockchain. DU logins onto the system and sends, an authorization 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 access requirement. DU receives the ciphertext, which includes ciphertext of data files and ciphertext of the symmetric key. 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.



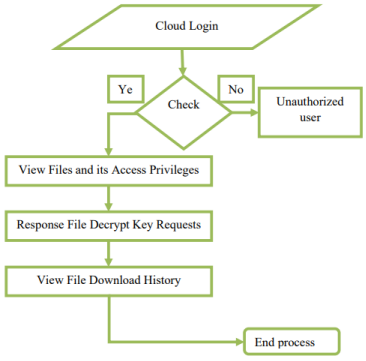
3. Data Owner:

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.



4. 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.



5. 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.

6. 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

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 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.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

The proposed identity authentication and key agreement protocol based on multi-layer blockchain was evaluated using metrics such as authentication time, key establishment latency, communication overhead,

computational cost, and security strength. Experimental results demonstrated that the protocol achieved secure mutual authentication and efficient session key generation with lower latency compared to conventional authentication methods. The multi-layer blockchain architecture improved scalability and reduced the burden on edge devices by distributing verification tasks across multiple layers.

The analysis showed that the protocol effectively resisted common security attacks such as replay attacks, impersonation attacks, and man-in-the-middle attacks while maintaining data confidentiality and integrity. Overall, the proposed approach provides a lightweight, secure, and scalable authentication solution suitable for edge computing and IoT environments.

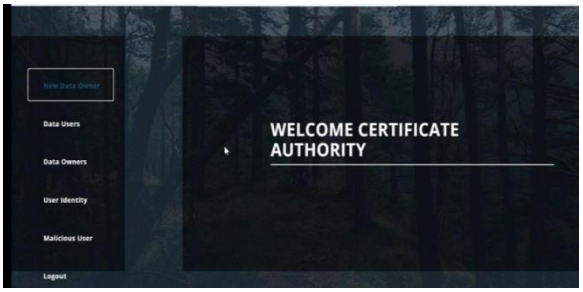


Fig. 2: Home Page

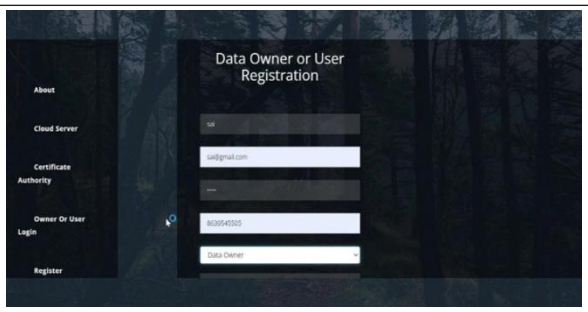


Fig. 3: Registration

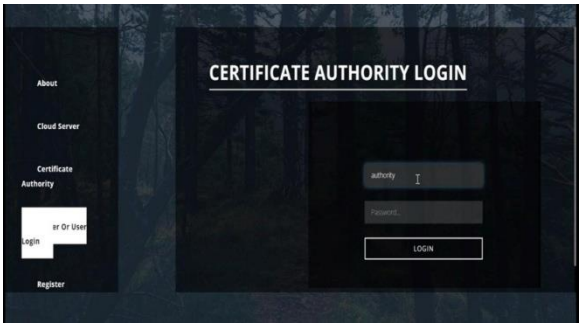


Fig. 4: Login

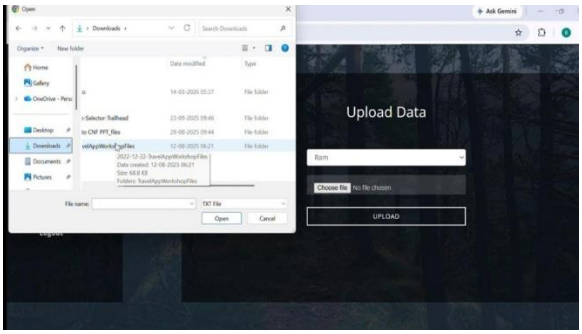


Fig. 5: Upload

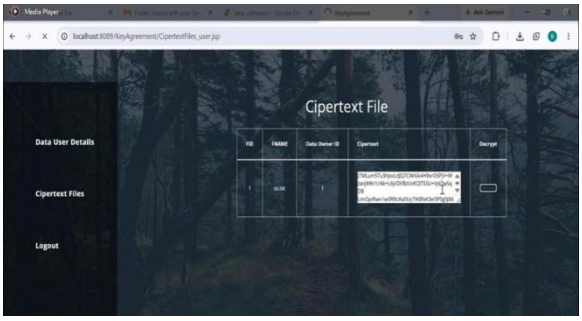


Fig. 5: Ciphertext File

V. 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.

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 IoTdriven 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.

AUTHORS Profile



Dr. NAVEEN REDDY NEMILI has received his MCA from Osmania University, Hyderabad in 2010, M.Tech degree in Computer science from JNTUH, Hyderabad in 2014 and Ph.D degree awarded in Computer Science from SSSUTMS, Madhyapradesh in 2024 He is dedicated to teaching field from the last 12 years. His research area Cloud Computing. At present he is working as Assistant Professor in CSE Department at Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India.



Mr. KAMBHAMPATI BHANU PRAKASH pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Ms. JEEDIPALLY SHARANYA pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. KAKARA RAMBABU pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. CHINNAM NARESH pursuing B.Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.