International Journal on Applications in Engineering and Technology
Volume 9 : Issue 2 : April 2023, pp 32 - 37 www.aetsjournal.com ISSN (Online) : 2455 - 0523

BLOCKCHAIN-BASED DECENTRALIZED AUTHENTICATION MODELING SCHEME IN EDGE AND IOT ENVIRONMENT

HEMALATHA . M , SUBADHARSHINI P

Abstract **-** The project **"BLOCKCHAIN-BASED DECENTRALIZED AUTHENTICATIONMODELING SCHEME IN EDGE AND IOT ENVIRONMENT "is** developed to Currently, Authentication is the first entrance to kinds of information systems; however, traditional centered single-side authentication is weak and fragile, which has security risk of single-side failure or breakdown caused by outside attacks or internal cheating. In the edge and IoT environmentblockchain can apply edge devices to better serve the Internet of Things and provide decentralized high security service solutions. In this paper, we proposed a blockchain-based decentralized authentication modeling scheme (named Block AUTH) in edge and IoT environment to provide a more secure, reliable and strong fault tolerance novel solution, in which each edge device is regarded as a node to form a blockchain network. We designed secure registration and authentication strategy, blockchain-based decentralized authentication protocol, and developed the blockchain consensus, smart contract, and implemented a whole blockchain-based authentication platform for the feasibility, security and performance evaluation. The analysis and evaluation show that the proposed Block AUTH scheme provides a more secure, reliable and strong fault tolerance decentralized novel authentication with high-level security driven configuration management. The proposed Block AUTH scheme is suitable for password-based, certificate-based, biotechnology-based, and token-based authentication for high level security requirement system in Edge and IoT Environment.

I. INTRODUCTION

As one of the most important entrances to kinds of information systems, authentication plays a prominent role in information system protection, which ensures the right user have access to the right system with the right identity. Currently, the identity authentication technologiesare consisting of 1) Password-based authentication. 2) Certificate-based authentication. 3) Biotechnology-based authentication, for instance, face, fingerprint or sound recognition.

As is known to all, the password-based authentication system stores the hash value of user's password in the database, and compares the current new password hash values with the stored hash of the original password. If they are consistent, the authentication is passed, otherwise the authentication will be rejected. Although the password-based authentication method is easy to achieve, some serious security problems are existed, such as the brute force cracking and the dictionary attack.

In order to ensure the identity information is not tampered and destroyed, Certificate-based authentication uses digital certificates in the authentication process, which is regarded as an extremely secure and reliable way. Digital certificate can effectively solve the problem of identity authentication in the network world by binding the identity information and related key of certificate holder. As the basic architecture of the digital certificate, Public Key Infrastructure (PKI) provides identity establishment and authentication mechanism in the network through digital certificates management, which allows users to use encryption, decryption technology and digital signature technology in various application scenarios easily.

And Biotechnology-based authentication collects users' biometric information, such as fingerprint, face, iris, voiceprint and so on, and compares them for identity information security. Biometric-based identification technology has many advantages over traditional identity authentication, for example, confidentiality, convenience, good anti-counterfeiting performance, not easy to forge or steal, carry around and use anytime and anywhere. However, the collection of biometric information is

M.Hemalatha , Assistant Professor , Department of Computer Applications , Erode Sengunthar Engineering College (Autonomous), Perundurai , Erode.

P.Subadharshini , PG Scholar , Department of Computer Applications, Erode Sengunthar Engineering College (Autonomous), Perundurai , Erode.

difficult. If the information is not encrypted, it may cause the leakage of private information.

Unfortunately, the current traditional authentication methods, such as the ones introduced above, are centralized schemes, which are weak and single-side with poor fault tolerance and reliability. Meanwhile, they have the following disadvantages:

1) The current single authentication has the hidden danger of single point failure, which is easy to be the target of the attacker, because the attacker can easily forge identity and others to implement the invasion.

2) Blindly trust the authentication agency will bring major security problems, the authentication agency may issue the wrong type of certificate, and are vulnerable to hacking, forgery, and falsification of digital certificates.

3) It is difficult for a single organization to provide multiple types of identity data on which comprehensive multi-factor authentication depends. Moreover, when a single organization is attacked, its corresponding local multi factor identity data can still be leaked. Obviously, in the centralized network, all management rights are gathered in the central node, which bears a huge risk because of the significant responsibility given.Since 2008, block chain technologies entered the public's vision with its unique characteristics of high transparency, decentralization, security and reliability. Up to now, many scholars have conducted in-depth research on the technology and security of block chain.

As far as the technological development trend of is concerned, the integration of the Internet of things (IOT) and the block chain is inevitable. Actually, IOT ensures that the information is accurate, real-time, transmitted, while the block chain establishes a trust mechanism by using its asymmetric encryption algorithm and time stamp technology, which can ensure the timeliness, security, and traceability of information in the process of transmission and sharing. Hence, in the process of merging the two technologies, IOT technology can provide more application scenarios for the block chain, while the block chain technology can solve the problems of information loss and privacy information security in the IOT.

At present, because of the centralized architecture, the traditional IOT system has great defects in security and robustness. Aiming at the problem, in this paper, we propose an identity authentication scheme based on block chain, called the Block Auth scheme, which uses edge devices to build block chain nodes and provides a decentralized, safe and reliable solution. Compared with traditional centralized authentication scheme in edge and IOT environment, our proposed scheme possesses three characteristics:

(1) Each edge device is regarded as a node to form a block chain network. All nodes of the decentralized network can participate in the management, and the relationship among nodes is equal. If one node fails, other nodes will replace it.

(2) The scheme can effectively avoid the traditional single-side fault. When the system authenticating a client user, the authentication unit is charged by the block chain nodes rather than the traditional centered authentication unit, which can avoid the single-side fault risk, especially when the traditional single authentication center is attacked or clasped because of heavy load.

(3) The Block Auth scheme is not only suitable for password-based authentication, but also suitable for certificate-based, bio-authentication,ortoken-based authentication, which can be used in high level security requirement, for instance, the core confidential or military system.

II. OBJECT DETECTION- AN OVERVIEW

The existing blockchain-based authentication scheme has the following shortcomings [21-23]. First, most of the existing schemes are built on the public chain, therefore, its reading and storage performance is low, the transaction time is long, its nodes are difficult to add or cancel flexibly, and the schemes are difficult to upgrade. Second, the existing scheme lacks the combination with the existing traditional InTechnology, so it is difficult to adapt to a variety of application scenarios. Third, some identity authentication schemes simply use the key technology, which is difficult to develop into the international standard general identity authentication schemes. Edge computing has important applications in distributed systems. In

order to further optimize the edge system, XiaofeiWang et al [25]. designed the "In-Edge AI" framework, proposed to integrate the Deep Reinforcement Learning techniques and Federated Learning framework with the mobile edge systems. In the Internet of things environment, each edge device can be regarded as a node to form a complete blockchain network, which realizes the integration of blockchain and Internet of things technology. This paper proposed the Block AUTH scheme combines the advantages of the above research ideas, and improves the shortcomings of the existing authentication schemes. It makes full use of the blockchain characteristics toile Internet of Things Journal, Volume:8, Issue:4, Issue Date: Feb.15,15.2021 ensure the privacy of identity information and the high transparency of authentication process, so that the authentication technology of this design scheme is credible and reliable in edge and IoT environment. III. THE BLOCKAUTH SCHEME A. The Block AUTH Scheme Model Fig. 1. The architecture of the Block AUTH Scheme In view of the problems existing in the current identity authentication protocol, a Block AUTH Scheme is proposed. In the proposed Block AUTH Scheme, the registration protocol, consensus mechanism of security enhancement and the authentication protocol are studied in detail.

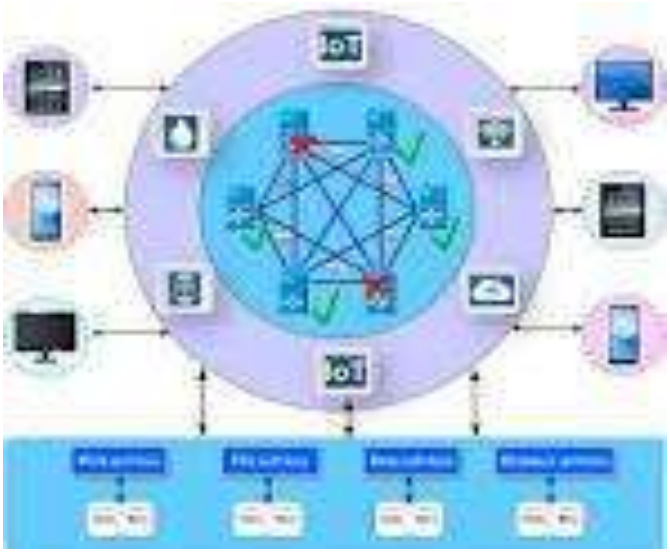

Figure: **The Block AUTHScheme Model**

The secure architecture of the Block AUTH scheme is described as Fig. 1. In the scheme, users can access data resources, service resources, business resources and management resources through the user interface, and can send user registration or authentication requests and information to the blockchain network. The blockchain network is the core of the platform, including smart contracts, node management, consensus mechanisms, cryptographic algorithms and other functions, providing secure services for all functions of the scheme. The business process of Block AUTH Scheme is shown in Fig. 2. In the service process, user can call the interface to send the request and data to the blockchain platform. Then, in order to deal with the request and data, the blockchain platform will call the blockchain execution engine to invoke the smart contract and other functions. After verification by at least three endorser nodes, the blockchain execution engine will call the block generation module to generate a new block. Finally, the engine will write the completed transaction into the newly created block, and write the timestamp and other information additionally.

III. LITERATURE SURVEY

The Internet of Things (IoT) or the cyberphysical system (CPS) is the network of connected devices, things, and people that collect and exchange information using the emerging telecommunication networks (4G, 5G IPbased LTE). These emerging telecommunication networks can also be used to transfer critical information between the source and destination, informing the control system about the outage in the electrical grid, or providing information about the emergency at the national express highway. This sensitive information requires authorization and authentication of source and destination involved in the communication. To protect the network from unauthorized access and to provide authentication, the telecommunication operators have to adopt the mechanism for seamless verification and authorization of parties involved in the communication. Currently, the next-generation telecommunication networks use a digest-based authentication mechanism, where the call-

processing engine of the telecommunication operator initiates the challenge to the request-initiating client or caller, which is being solved by the client to prove his credentials. However, the digest-based authentication mechanisms are vulnerable to many forms of known attacks, e.g., the man-in-the-middle (MITM) attack and the password guessing attack. Furthermore, the digest-based systems require extensive processing overheads. Several publickey infrastructure (PKI)-based and identity-based schemes have been proposed for the authentication and key agreements. However, these schemes generally require a smart card to hold long-term private keys and authentication credentials. In this article, we propose a novel self-enforcing authentication protocol for the session-initiation-protocolbased next-generation network, based on a low-entropy shared password without relying on any PKI or the trusted third party system.

IV. SYSTEM ANALYSIS

For the research of edge computing, many scholars also put forward different solutions. To address the complex and dynamic control issues, Xiaofei Wang et al. proposed a Federated Deep reinforcement learning-based cooperative Edge caching (FADE) framework.

In 2008, blockchain came into the public's view. Blockchain is a combination of encryption algorithm, consensus mechanism, distributed data storage and point-to-point transmission, which has the characteristics of transparency, immutability, anonymity and high security. With the implementation of blockchain, scholars realized that blockchain technology can be used not only in the field of economics and currency, but also in the field of security control. Identity authentication and access control based on blockchain have been widely concerned and studied. Research on blockchain-based schemes improved authentication methods much more.

Dugard A et al. proposed a blockchain-based decentralized network trust and IoT authentication protocol under the public key encryption system. Sandal, Tomoyuki. etal. proposed a new authentication method in Wi-Fi access using Bitcoin 2.0. Punthali D et al. presented a novel consensus algorithm called Proof-of-Authentication (Poach) to replace Proof-of-Work and introduce authentication. H.Es-Samaliet al. contributed to reinforcing the security of Big Data platforms by proposing a blockchain-based access control framework.

The existing blockchain-based authentication scheme has the following shortcomings. First, most of the existing schemes are built on the public chain, therefore, its reading and storage performance is low, the transaction time is long, its nodes are difficult to add or cancel flexibly, and the schemes are difficult to upgrade. Second, the existing scheme lacks the combination with the existing traditional PKI technology, so it is difficult to adapt to a variety of application scenarios. Third, some identity authentication schemes simply use the key technology, which is difficult to develop into the international standard general identity authentication schemes. Edge computing has important applications in distributed systems. In order to further optimize the edge system, Xiaofei Wang et al. designed the “In-Edge AI” framework, proposed to integrate the Deep Reinforcement Learning techniques and Federated Learning framework with the mobile edge systems.

DISADVANTAGES

1) The current single authentication has the hidden danger of single point failure, which is easy to be the target of the attacker, because the attacker can easily forge identity and others to implement the invasion.
2) Blindly trust the authentication agency will bring major security problems, the authentication agency may issue the wrong type of certificate, and are vulnerable to hacking, forgery, and falsification of digital certificates.
3) It is difficult for a single organization to provide multiple types of identity data on which comprehensive multi-factor authentication depends. Moreover, when a single organization is attacked, its corresponding local multi-factor identity data can still be leaked.

V. PROPOSED SYSTEM

At present, because of the centralized architecture, the traditional IoT system has great defects in security and robustness. Aiming at the problem, in this paper, we propose an identity authentication scheme based on blockchain, called the Block AUTH scheme, which uses edge devices to build blockchain nodes and provides a decentralized, safe and reliable solution. Compared with traditional centralized authentication scheme in edge and IoT environment, our proposed scheme possesses three characteristics:

(1) Each edge device is regarded as a node to form a blockchain network. All nodes of the decentralized network can participate in the management, and the relationship among nodes is equal. If one node fails, other nodes will replace it.

(2) The scheme can effectively avoid the traditional single-side fault. When the system authenticating a client user, the authentication unit is charged by the blockchain nodes rather than the traditional centered authentication unit, which can avoid the single-side fault risk, especially when the traditional single authentication center is attacked or clasped because of heavy load.

(3) The Block AUTH scheme is not only suitable for password-based authentication, but also suitable for certificate-based, bio-authentication, or token-based authentication, which can be used in high level security requirement, for instance, the core confidential or military system.

ADVANTAGES

(1)Propose. The client sends the request message *m* to the nodes in the network, including the leader node and other endorser nodes.

(2)Pre-prepare. The leader node receives the request message *m* sent by the client, assigns the *m* serial number *s*, and calculates the pre-prepare message (*pre-prepare*, H (m), *s*, *v*), where H () is a one-way hash function, and *v* represents the view at this time. Before sending a message, the node needs to digitally sign *m* with its private key. Then the leader node sends the prepared message to other endorser nodes in the organization.

VI. SYSTEM IMPLEMENTATION

1) DATA OWNER

In this module, the Owner acts as Service Provider browses the required file, initializes nodes with digital signature and uploads to the end user (node a, node b, node c, node d, node e, node f) via Router and performs the following operations Init mac for all packets, Encrypt Upload data.

2) BLOCK CHAIN ROUTER

The BC Router is responsible for forwarding the data file in shortest distance to the destination; the BC Router consists of Group of nodes, the each and every node (n1, n2, n3, n4, n5, n6, n7, n8, n8, n10, n11, n12, n13) consist of Bandwidth and Digital Signature. If BC router had found any malicious or traffic node in the router then it forwards to the CA and performs the following operations such as Initialize mac for all packets and nodes, Receive Data, Find Path based on the distance and check attackers, if attacker found and send to ids manager, apply localization technique to avoid attackers ,Finally verify whether the user is registered in the data owner or not. If user is no authorized then inform to data owner, Find Time delay and energy, Capture the attacker Ip address, Viewattackers, nodes, distance.

3) CA

The CA manager is nothing but Intrusion Detection System manager which is responsible to filter the malicious data and traffic data. The CA manager decides the phases based on BC Router status and then decides on type oak attackers

4) RECEIVERS/END USERS

In this module, the End user can receive the data file from the Service Provider which is sent via BC Router, if malicious or traffic node is found in the router then it forwards to the CA Manager to filter the content and adds to the attacker profile.

5) ATTACKER

In this module, the malicious node or the traffic node details can be identified by a threshold-based classifier is employed in the Attack Detection module to distinguish DoS attacks from legitimate

traffic. The Attacker can inject the fake message and generates the signature to a particular node in the router with the help of threshold-based classifier in testing phase and then adds to the attacker profile.

VII. CONCLUSION

In order to solve the security and reliability of traditional authentication in the edge and IOT environment, we proposed a Block Auth Scheme, which can provide a more secure, reliable and strong fault tolerance decentralized novel authentication solution with high-level security. In this scheme, each edge device is regarded as a node to form block chain network. Specially, we designed the secure registration and authentication strategy and the block chain-based decentralized authentication protocol, improved the block chain consensus, developed smart contract, and finally implemented the whole block chain-based authentication platform for the feasibility, security and performance evaluation. According to Evaluations and Comparison with the existing related scheme, our scheme enhances security and stability on the basis of sacrificing a certain degree of time complexity, and meets the high security and fault tolerance requirements of identity authentication in edge and IOT environment. Furthermore, this scheme proposed by us can meet the authentication requirements of multiple scenarios and development demand of the international standard authentication scheme.

VIII. REFERENCES

[1] Proc. Roy. Soc. A Math. Phys. Eng. Sci., vol. 426, no. 1871, pp. 233-271, 1989.

[2] M. Abadi and M. R. Tuttle, "A semantics for a logic of authentication", Proc. 10th Annu. ACM Sump. Prince. Diatribe. Compute., pp. 201-216, 1991.

[3] Hung-Yu Chien. SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity. IEEE Transactions on Dependable and Secure Computing, vol.4, pp.227 340, 2007.

[4] Jia-Lunn Tsai; Nai-Wei Lo. A Privacy-Aware Authentication Scheme for Distributed Mobile Cloud Computing Services. IEEE Systems Journal, vol.9, pp.805-815, 2015.

[5] Muhammad Ajmal Azad; Samira Bag; Cherith Perera; Mahmoud Brahimi; Feng Hao. Authentic Caller: Self-Enforcing Authentication in a Next-Generation Network. IEEE Transactions on Industrial Informatics, vol.16, pp.3606-3615,2020.

[6] Libor Dostaler. Multi-Factor Authentication Modeling. 2019 9th International Conference on Advanced Computer Information Technologies (ACIT).

[7] K. M. Renuka; Saru Kumari; Donning Zhao; Li Li. Design of a Secure Password-Based Authentication Scheme for M2M Networks in IoT Enabled Cyber-Physical Systems. IEEE Access, vol.7, pp. 51014 – 51027, 2019.

[8] T.-D. Nguyen, A. Al-Safar and E.-N. Huh, "A dynamic id-based authentication scheme", Proc. 6th Int. Conf. Newt. Compute. Adv. Inf. Manage. (NCM), pp. 248-253, Aug. 2010.

[9] S. Chen, M. Ma and Z. Luo, "An authentication scheme with identity-based cryptography for M2M security in cyber-physical systems", Secure. Commune. Newt., vol. 9, pp. 1146-1157, 2016.

[10] X. Sun, S. Men, C. Zhao and Z. Zhou, "A security authentication scheme in machine-to-machine home network service", Secure. Commune. Newt., vol. 8, no. 16, pp. 2678-2686, 2015.

[11] Arno Fiedler, Christoph Thiel. Certificate Transparency. Mateschitz und Datensicherheit - Dud, 2014, Vol.38 (10), pp.679-683.

[12] Swan M. Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc., 2015.

[13] Ryan Henry; Amir Herzberg; Aniket Kate, "Blockchain Access Privacy: Challenges and Directions", IEEE Security & Privacy, vol.16, no.4, pp.38-45,2018.

[14] Tomaso Aster; Paolo Tascam; Tatiana Di Matteo, "Blockchain Technologies: The Foreseeable Impact on Society and Industry", Computer, vol.50, no.9, pp.18-28,2017.

[15] Tien Tuan Anh Dinh; Rui Liu; Meihui Zhang. "Untangling Blockchain: A Data Processing View of Blockchain Systems", IEEE Transactions on Knowledge and Data Engineering, vol.30, no.7, pp.1366-1385,2018.

[16] H. G. Do, W. K. Ng, "Blockchain-based system for secure data storage with private keyword search", 2017 IEEE World Congress on Services (SERVICES), pp. 90-93, 2017.

[17] Y Zhi, Y Kan, et.al. Blockchain-based Decentralized Trust Management in Vehicular Networks, IEEE Internet of Things Journal, Vol.6, No.2, pp.1495-1505,2019.

[18] Xu Q, Jinn C, Rasid M F B M, et al. Blockchain-based decentralized content trust for docker images. Multimedia Tools and Applications, Vol.77, No.14, pp.18223–18248,2018.

[19] Dugard A, Gremaud P, Pesquera J. Decentralized web of trust and authentication for the internet of things. Proceedings of the Seventh International Conference on the Internet of Things. ACM, 2017: 27.

[20] Sandal T, Inaba H. Proposal of new authentication method in Wi-Fi access using bitcoin 2.0. Consumer Electronics, 2016 IEEE 5th Global Conference on. IEEE, 2016:1-5.

[21] S. Khan and R. Khan, "Multiple authorities attribute-based verification mechanism for Blockchain microgrid transactions," Energies, vol. 11, no. 5, p. 1154, 2018.

[22] Punthali D, Mohanty SP, Nanda P, Koulianos E, Das G. Proof-of-authentication for scalable blockchain in resource-constrained distributed systems. In: Proceedings of the 2019 IEEE international conference on consumer electronics (ICCE). IEEE; 2019. p. 1–5.

[23] H. Es-Samali, A. Outthought, and J. P. Leroy, A blockchain-based access control for big data, Int. J. Compute. Newt. Commune. Secure., vol. 5, no. 7, pp. 137–147, 2017.

[24] Xiaofei Wang, Shenyang Wang, Xinhua Li, Victor C. M. Leung, Tarik Talab: Federated Deep Reinforcement Learning for Internet of Things with Decentralized Cooperative Edge Caching. IEEE IoT Journal, DOI: 10.1109/JIOT.2020.2986803

[25] Xiaofei Wang, Yawen Han, Shenyang Wang, Qi yang Zhao, Xu Chen, Min Chen: In-Edge AI: Intelligent zing Mobile Edge Computing, Caching and Communication by Federated Learning. IEEE Network 33(5): 156-165 (2019)