International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 13, Issue 2, 2025

A New Identity Authentication And Key Agreement Protocol Based On Multi-Layer Blockchain In Edge Computing

Manik Rao Patil, S.Akshay, Sr.Vinay Anand, Krv.Karthik

[1]Assistant Professor, Department Of IT, Guru Nanak Institutions Technical Campus (Autonomous), India.

[2,3,4]B.Tech Students, Department Of IT, Guru Nanak Institutions Technical Campus (Autonomous), India

akshaysoma3727@gmail.com

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.

1-INTRODUCTION

Nowadays, we are witnessing the rapid proliferation of intelligent devices in the digital age, ushering in an era of interconnected everything [1]. The IoT exhibits characteristics such as multi-source heterogeneity and openness, but it also confronts challenges related to cyber threats and privacy [2]. 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 [3], smart cities [4], intelligent transportation [5], healthcare [6], and the industrial Internet of Things [7]. 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 [8] 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) [12]. 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.

2-LITERATURE SURVEY

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

Year: 2023

Author: A. Islam and S. Y. Shin.

Description: 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 [1]. 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.

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: 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.

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: 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.

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 ever-increasing requirements of delay-sensitive and mission-critical applications, it becomes a popular research trend to incorporate edge computing in the Internet of Things (IoT) to mitigate the pressure of traditional cloud-based IoT architecture. Edge computing delivers real-time computations and communications for IoT devices by leveraging edge servers deployed close to users, which creates a collaborative edge computing (CEC) paradigm. The capacity of edge servers is beneficial but risky, as vulnerable servers can be exploited to

conduct surveillance or perform other nefarious activities. Besides, fake IoT devices would bring security threats and compromise the IoT system. This highlights the necessity of designing a secure and efficient mutual authentication scheme for CEC. In this direction, related works have proposed various authentication mechanisms, but most of them are found unfit due to the absence of decentralization, anonymity, and mobility. Motivated by this fact, we propose a blockchain-based mutual authentication scheme that bridges these gaps. Specifically, blockchain, certificate less cryptography, elliptic curve cryptography, and pseudonym-based cryptography are integrated into our scheme to provide mutual authentication between edge servers and IoT devices. Except for static conditions, both intraedge and interedge authentication are considered. Besides, we elaborate on the key generation procedures and design a session key negotiation mechanism. Extensive experiments and security analyses have been conducted to show the feasibility of the proposed scheme.

Due to closer communication distance, end-users are able to enjoy services with lower latency and higher bandwidth. Besides, edge computing's distributed structure can balance network traffic and prevent the traffic peaks in IoT networks. Furthermore, by offloading computation-intensive tasks from resource-limited IoT nodes to edge servers with relatively significant resources, the system can extend the lifetime of individual nodes.

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 represent two key components for network management, especially to guarantee the trusted operation of massive access networks such as the Internet of Things (IoT). As a core technology to provide low latency and high communication for IoT, Mobile Edge Computing (MEC) pulls computing resources from remote cloud centers to devices. The process of MEC service involves three types of entities: devices, data generated by devices and digital evidence generated after the data interaction. These entities are fully distributed and difficult to protect through traditional, highly centralized security and authentication mechanisms. As a decentralized shared ledger and database, the emerging blockchain is considered to provide cooperative trust and collaborative action among multiple subjects while ensuring the integrity and confidentiality of data. Because of its anonymity, non-tampering and traceability, the blockchain arouses research on the combination of blockchain and edge computing for device security, data security and forensics in IoT. This survey analyzes the application of blockchain in MEC-IoT systems and mainly focuses on approaches and technologies to manage the security and forensics issues for IoT. Finally, we present open issues and prospects for future work and research directions.

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:
Recently, the Digital Twin (DT) technology has procured a lot of attention because of its applicability in the manufacturing and space industries. The DT environment involves the formation of a clone of the tangible object to perform simulations in the virtual space. The combination of conceptual development, predictive maintenance, real-time monitoring, and simulation characteristics of DT has increased the utilization of DT in different scenarios, such as medical environments, healthcare, manufacturing industries, aerospace, etc. However, these utilizations have also brought serious security pitfalls in DT deployment. Towards this, several authentication protocols with different security and privacy features for DT environments have been proposed. In this article, we first review a recently proposed two-factor authentication protocol for DT environments that utilizes the blockchain technology. However, the analyzed scheme is unable to offer the desirable security and cannot withstand various security attacks like offline password-guessing attack, smart card stolen attack, anonymity property, and known session-specific temporary information attack. We also demonstrate that an attacker can impersonate the analyzed protocol's legal user, owner, and cloud server. To mitigate these security loopholes, we devise an effective three-factor privacy-preserving authentication scheme for DT environments. The proposed work is demonstrated to be secure by performing the informal security analysis, the formal security analysis using the widely recognized Burrows-Abadi-Needham (BAN) logic, and the Real-or-Random (ROR) model. A detailed comparative study on existing competing schemes including the analyzed scheme demonstrates that the devised framework furnishes better security features while also having lower computation costs and comparable communication costs than the existing schemes.

Cloud computing is the most feasible approach for implementing DT services since it has prodigious advantages. It provides on-demand services, computing resources, ubiquitous network access,

etc., making it suitable for the next-generation information technology architecture. In cloud-assisted DT environments, the data owners generate data from physical assets and disseminate it to the cloud server, simulating DT in virtual space and sharing the simulation results with the owner. At the same time, the user can access the data upon request. However, putting DT technology into practice faces several obstacles. The biggest challenge is finding a secure way to share simulation and real-time data. Serious privacy implications are to be faced if the sensitive information transmitted by the data owner gets held by the adversary. Evidently, the below-illustrated points are necessary for the deployment of DT environment: (a) There is a strong urge to develop a secure medium for efficiently sharing the transmitted data. (b) There must be a procedure for validating the transmitted data; that is, verification of data integrity is required. (c) Security prerequisites such as untraceability, anonymity, and confidentiality should be guaranteed.

To achieve the aforementioned security prerequisites, we need a secure and privacy-preserving authentication protocol employing the benefits of blockchain technology. With blockchain, the data owner or user who utilizes data is allowed to verify the integrity of the data Users may readily validate the requested data using a Merkle hash tree. The framework proposed in this paper utilizes a cloud server to store the DT data and blockchain for the data hash values, enabling the users to verify the integrity of received data. Furthermore, the log transactions of shared data among the user-server are uploaded to the blockchain.

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, engagement in various remote activities such as online education and meetings has increased. However, since the conventional online environments typically provide simple streaming services using cameras and microphones, there have limitations in terms of physical expression and experiencing real-world activities such as cultural and economic activities. Recently, metaverse environments, three-dimensional virtual reality that use avatars, have attracted increasing attention as a means to solve these problems. Thus, many metaverse platforms such as Roblox, Minecraft, and Fortnite have been emerging to provide various services to users. However, such metaverse environments are potentially vulnerable to various security threats because the users and platform servers communicate through public channels. In addition, sensitive user data such as identity, password, and biometric information are managed by each platform server. In this paper, we design a system model that can guarantee secure communication and transparently manage user identification data in metaverse environments using blockchain technology. We also propose a mutual authentication scheme using biometric information and Elliptic Curve Cryptography (ECC) to provide secure communication between users and platform servers and secure avatar interactions between avatars and avatars. To demonstrate the security of the proposed mutual authentication scheme, we perform informal security analysis, Burrows–Abadi–Needham (BAN) logic, Real-or-Random (ROR) model, and Automated Validation of Internet Security Protocols and Applications (AVISPA). In addition, we compare the computation costs, communication costs, and security features of the proposed scheme with existing schemes in similar environments. The results demonstrate that the proposed scheme has lower computation and communication costs and can provide a wider range of security features than existing schemes. Thus, our proposed sche.

3-PROJECT DESCRIPTION

The cross-domain certificate revocation mechanism was designed to improve the authentication efficiency. Proposed 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. Focused on the authentication between different security domains in IoT. A master-slave blockchain architecture supporting distributed cross-domain authentication was designed. 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.

METHODOLOGIES

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**
- **Multi-Layer Blockchain Provides**

MODULES EXPLANATION AND DIAGRAM

- **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.

Cloud Server

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.

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.

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.

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.

4-REQUIREMENTS ENGINEERING

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis, the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.

Three key considerations involved in the feasibility analysis are

ECONOMICAL FEASIBILITY: This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus, the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

TECHNICAL FEASIBILITY: This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

SOCIAL FEASIBILITY: The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of the system.

HARDWARE REQUIREMENTS

The hardware requirements may serve as the basis for a contract for the implementation of the system and should therefore be a complete and consistent specification of the whole system. Software engineers use them as the starting point for the system design. It shoulds what the system and not how it should be implemented.

SOFTWARE REQUIREMENTS

The software requirements document is the specification of the system. It should include both a

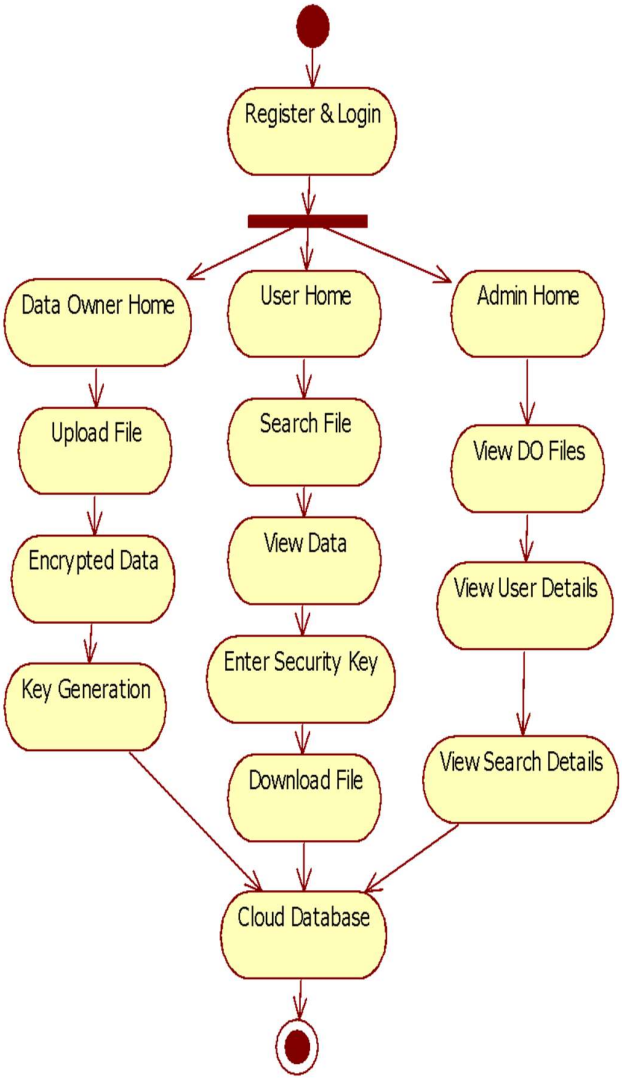
International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025

definition and a specification of requirements. It is a set of what the system should do rather than how it should do it. The software requirements provide a basis for creating the software requirements specification. It is useful in estimating cost, planning team activities, performing tasks, tracking the teams, and tracking the team's progress throughout the development activity.

5-DESIGN ENGINEERING

Design Engineering deals with the various UML [Unified Modelling language] diagrams for the implementation of project. Design is a meaningful engineering representation of a thing that is to be built. Software design is a process through which the requirements are translated into representation of the software. Design is the place where quality is rendered in software engineering. Design is the means to accurately translate customer requirements into finished product.

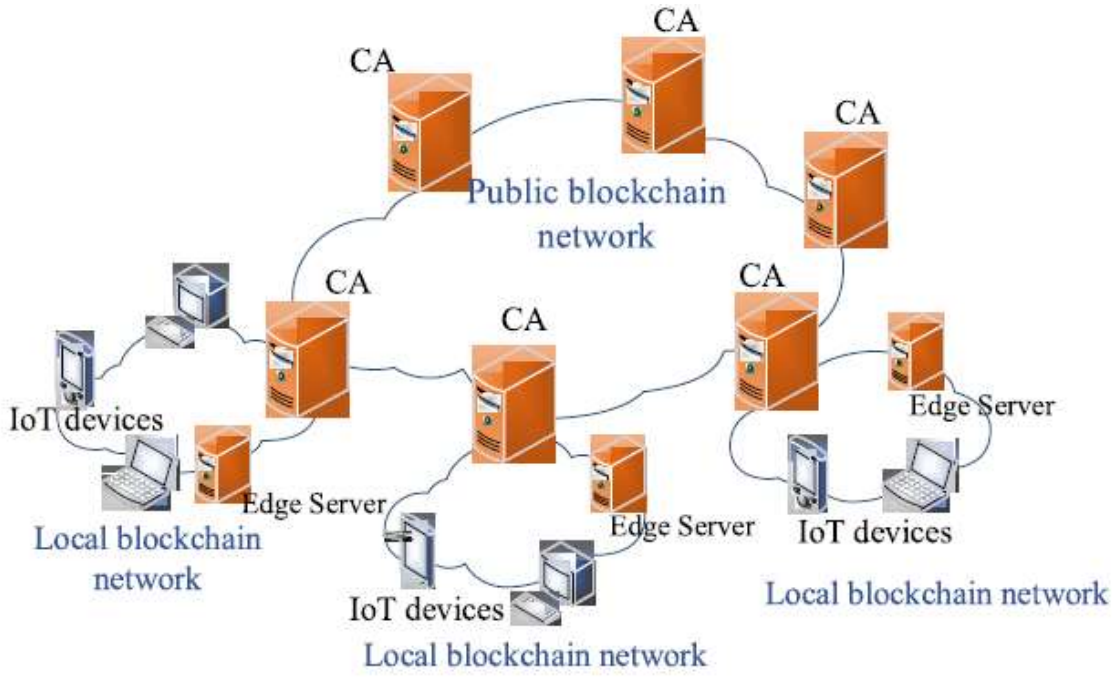
Activity Diagram



Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. In the Unified Modeling Language, activity diagrams can be used to describe the business and operational step-by-step workflows of components in a system. An activity diagram shows the overall flow of control.

System Architecture

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025



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.

6-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.

REFERENCE

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.
18. A. 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. C. 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. D. 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. D. 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.
40. FISCO-BCOS, Oct. 2020, [online] Available: https://wwwfisco-bcos.org.