Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2025 SCPE. Volume 26, Issues 1, pp. 180–190, DOI 10.12694/scpe.v26i1.3785

# FINE-GRAINED TRUSTED CONTROL METHODS FOR IOT BOUNDARY ACCESS

JIE WANG[*] CHANG LIU[†] GUOWEI ZHU[‡] XIAOJUN LIU[§] AND BIBO XIAO[¶]

**Abstract.** In order to solve the problems of coarse-grained access policies, weak auditability, lack of access process control, and excessive privileges exhibited by existing IoT access control technologies, the author proposes a fine-grained trusted control method for IoT boundary access. The author elaborated on the CcBAC model framework and formalized its definition; At the same time, specific descriptions of the functions in the model were provided, and the access control process of this model in general application scenarios was presented; After rigorous testing, it was found that as the number of requests increased, there was a slight uptick in the average time it took for the function to process them, but beyond a certain point, this time plateaued and even began to decrease gradually. Meanwhile, the system's throughput increased steadily with more requests until it reached a stable level, showing no significant drop even with additional clients. The proposed CcBAC access control model showcased remarkable performance in handling large-scale requests while ensuring fine-grained, autonomous authorization, security, and auditability. It effectively achieved consensus in distributed systems and maintained data consistency. In conclusion, this model empowers resource owners with full control over their resources' access, while also accounting for the detailed and traceable nature of access control.

**Key words:** Blockchain, Access control, Internet of Things, Cryptocurrency, Trusted Execution Environment

## 1. Introduction.

With the development and maturity of Internet of Things technology, it has gradually evolved from an initial concept and penetrated into various fields, such as intelligent transportation, medical care, environmental monitoring, and other multi industry fields [1]. Billions of IoT devices have begun to be widely used in people's social lives, generating exponential growth in IoT data. The era of data has arrived. The Internet of Things data is the core driving force behind the Internet of Things, containing enormous value, and the most important way to unleash the value of data is to make it flow. In order to accelerate the process of data sharing and circulation, and better serve various fields such as education, business, and infrastructure, in recent years, the country has elevated the construction and development of data to a national strategy and actively transitioned towards a digital economy [2]. In October 2020, the Central Committee of the Communist Party of China unveiled the "14th Five-Year Plan for National Economic and Social Development." This plan emphasized the imperative of advancing the utilization of data and information resources, with a specific goal of fostering open sharing of fundamental information. In March 2021, the State Council released the Government Work Report, which mentioned the need to improve data sharing coordination capabilities and improve data sharing coordination mechanisms [3]. Driven by policies, there is an increasing amount of research on data sharing in the Internet of Things, and a number of data sharing application cases have emerged. However, due to the fact that most solutions adopt a centralized data management model, the degree of sharing is low, and data cannot be monetized, so the value of data cannot be released. The reason behind this is that there are currently many problems exposed in the process of data sharing transactions, lacking a reliable, open and transparent data sharing atmosphere [4]. Blockchain, relying on features such as decentralization, difficulty in tampering, and traceability of transactions, provides the possibility of building a reliable and transparent IoT data sharing environment.

## 2. Literature Review.

As a new decentralized, trustworthy, and tamper proof technology, blockchain can provide a trusted implementation solution for trust and data security issues in the field of data sharing.

[*] State Grid Hubei Electric Power Research Institute, Hubei Wuhan, 430077, China (Corresponding author, JieWang59@163.com)

[†] State Grid Hubei Electric Power Research Institute, Hubei Wuhan, 430077, China (ChangLiu61@126.com)

[‡] State Grid Hubei Electric Power Co., Ltd, Hubei Wuhan, 430077, China (GuoweiZhu7@163.com)

[§] State Grid Yichang Power Supply Company, Hubei Yichang, 443000, China (XiaojunLiu8@126.com)

[¶] State Grid Yichang Power Supply Company, Hubei Yichang, 443000, China (BiboXiao6@163.com)

Therefore, the combination of blockchain technology and IoT data sharing has become a research hotspot in the academic community [5].

The characteristics of blockchain can provide an auditable platform for data sharing, such as recording the data sharing process on the chain, providing a data foundation for subsequent service evaluation. The combination of blockchain and the Internet of Things has received considerable academic research, and in the field of data sharing, blockchain mainly focuses on protecting the confidentiality, integrity, and availability of data. Atlam, H. F. et al. introduced an innovative IoT technology access control model centered around risk assessment, catering to real-time data requests from IoT devices while offering dynamic responsiveness. This model leverages IoT environment attributes to gauge security risks linked to access requests, employing factors such as user context, resource sensitivity, action severity, and past risk records to inform its security risk estimation algorithm, pivotal for access control decisions. Moreover, the model integrates smart contracts to enable adaptability, actively monitoring authorized user conduct to swiftly identify any irregular behaviors[6]. Wang et al. introduced an access control approach tailored for laboratory cloud data, integrating Internet of Things (IoT) technology. The method breaks down laboratory cloud database data into minimal attributes, encrypting them and creating a key of minimal granularity that adheres to access tree constraints. By combining IoT and proxy re-encryption technologies, the method maps access structures and attribute sets using hash functions, encrypts symmetric keys via the CP-ABE scheme, and facilitates laboratory cloud scalability based on access control methodologies[7]. Conventional centralized data sharing systems pose risks like single points of failure and overburdened central nodes. To address these challenges and foster a more distributed and collaborative approach, researchers have increasingly turned to blockchain-based solutions for Internet of Things (IoT) environments. However, without predefined policies, legitimate user access may be denied, and data updates on the blockchain may bring high costs to owners. Wang, R. et al. addressed these challenges by integrating the Accountable Subgroup Multiple Signature (ASM) algorithm with Attribute Based Access Control (ABAC) techniques, along with policy smart contracts. This fusion delivers a precise and adaptable solution, offering detailed control over access permissions [8].

Traditional models such as RBAC, ABAC, and CapBAC have limitations in fine-grained control, policy flexibility, and auditability, while blockchain based access control schemes have significant advantages in data immutability and decentralization, despite advancements, there are opportunities to enhance policy articulation and execution speed. To address these, the author introduces a novel access control model leveraging cryptocurrency and trusted execution environments (CcBAC). This model automates policy determination and transparently executes them via blockchain, while ensuring secure off-chain policy execution through trusted execution environments (TEE). The CcBAC model not only solves the application problems of existing methods in the Internet of Things environment, but also provides new ideas and methods for future related research. Through this combination, we aim to provide a more secure, flexible, and auditable access control solution for IoT devices.

## 3. Research Methods.

**3.1. CcBAC Access Control Model.** The CcBAC access control model is a universal access control model that uses the cryptocurrency Ccoin to represent access permissions. The purpose of Ccoin is to concretize access capabilities into atomic, trustworthy, and transferable digital assets. The core idea is to establish a unified standard to describe the permission control policies of each resource through deep integration of trusted execution environment and blockchain technology, in order to achieve fine-grained and dynamic management of policies and provide convenience for user access. Using blockchain networks as interaction media, driven by smart contracts, to achieve automated decision-making of access policies, authentic and trustworthy execution, transparent and traceable access processes, and auditable policy execution processes. By introducing trusted access control objects, control over the access process is achieved to prevent excessive privileges; Meanwhile, any user can independently formulate access policies to achieve flexible management and sharing of resources.

In this model, Ccoin is a cryptocurrency used for access control, which is used to verify and authorize user access to resources. Each Ccoin contains access policies and metadata to achieve fine-grained access control. Ccoin plays the following roles in access control security:

1) Fine grained control: Each Ccoin includes access policies that can define specific access permissions and restrictions. Through Ccoin, fine-grained control of resources can be achieved, allowing only authorized

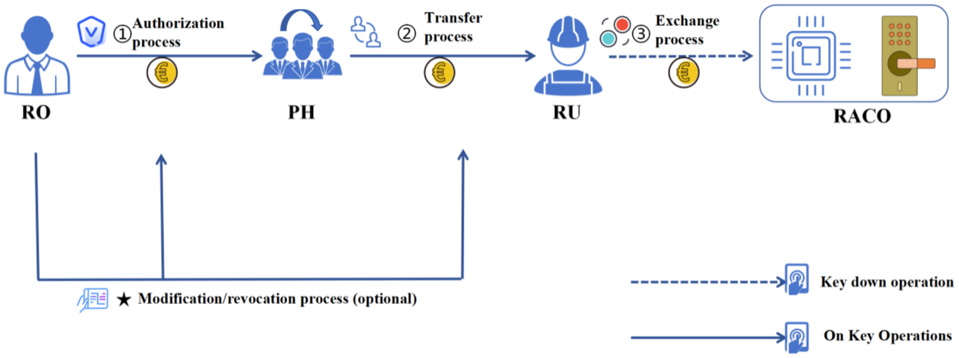

Fig. 3.1: Access Control Model Based on Ccoin

users to perform specific operations [9].

2) Auditability: The operations and resource access activities of Ccoin are recorded in blockchain transactions to ensure auditability. This means that all operations and access activities are public, verifiable, and traceable.
3) Access process control: Through Ccoin, control over the access process can be achieved. Before accessing resources, a verification and authorization process is required to ensure that users meet the access conditions. At the same time, Ccoin can also record activities during the access process for auditing and control.
4) Preventing Witch Attacks: Ccoin can effectively prevent witch attacks through the decentralized nature of blockchain technology.
5) Secure storage: The operations and access activities of Ccoin are recorded in the transactions of the blockchain, which means that Ccoin's data is stored in a distributed network. Compared to traditional centralized storage, distributed storage has higher security and reliability.

The access strategy consists of five key fine-grained elements that determine the access control scheme: In access control terminology, the ”4W1H access policy” refers to specifying the ”who, what, where, when, and how” of access permissions. Essentially, it outlines the conditions necessary for granting access requests. The ”who” identifies the authorized users, the ”what” specifies the actions they are permitted to perform, the ”where” indicates the locations where access is granted, and the ”when” delineates the time frames for access. Finally, the ”how” details the precise process that must be adhered to during the access period. The 4W1H access policy is forged into the digital currency Ccoin, and all operations against Ccoin will be securely recorded for review throughout its entire lifecycle. Before the Ccoin is redeemed, resource owners can modify or revoke access policies in the Ccoin to achieve fine-grained control over resource access permissions[10]. This approach exhibits four distinct traits:

1) Sole Authority: Only resource owners possess the ability to create, modify, and revoke Ccoins.
2) Transferability: Holders of Ccoins can freely transfer them to other participants.
3) Conditional Redemption: Ccoin redemption is contingent upon meeting access policy conditions, with strict adherence required for resource access.
4) Immutable Recording: All access actions are securely logged on the blockchain for auditing purposes. The model facilitates interactions between Resource Owners (RO), Resource Requesters (RU), Permission Holders (PH), and Reliable Access Control Objects (RACO), with each entity identified by distinct addresses. Participants possess individual wallets containing Ccoins, representing access permissions. Transactions within this model primarily encompass three steps, as illustrated in Figure 3.1.

The trusted access control object, RACO, serves as a dependable module representing the interests of resource owners. Its responsibilities include verifying the functional integrity of Ccoin, ensuring compliance with fine-grained access conditions, making access decisions, and monitoring the access process [11]. To ensure the trustworthiness and security of RACO, it is housed within a trusted execution environment (TEE). TEE offers a secure processing environment that is resistant to tampering, allowing for secure isolation and storage within the chipset. Its core functionalities include secure startup, runtime isolation, secure storage, scheduling, trusted I/O operations, and remote management. TEE can ensure the authenticity, integrity, and confidentiality of RACO code and runtime status, and resist software attacks and physical tampering.

### 3.2. Basic Elements and Functions.

*Definition 1.* CcABC defines the cryptocurrency representing access rights as Ccoin, denoted as c=(tokenId, owner, holder, device, policy, timestamp, isValid).

This approach leverages blockchain technology to ensure secure data storage and atomic data transmission, with consensus among participating nodes maintaining ledger consistency. Ccoin transactions take place on the blockchain, with operations such as createCcoin, transferFrom, updatePolicy, revokeCcoin, and redeemCcoin initiated by sending messages to all blockchain nodes. Ensuring authenticity, the function caller must sign the message using a key. In CcBAC, the message format of the caller's public key infrastructure (pki) is formatted as follows 3.1:

$$msg : [tokenId, op, \{policy\}, \{pk_j\}]_{\sigma_{pk_i}} \tag{3.1}$$

Among them, op represents the operation code of the function, and optional information is enclosed in curly braces. If op=createCcoin or updatePolicy, $\{policy\}$ holds a valid policy; If op=transferFrom, then $\{pk_j\}$ is the new recipient public key. $\sigma_{pk_i}$ represents the key signature of the function caller $pk_j$.

System participants include both regular blockchain nodes and users who interact with the blockchain through secure channels. When participants engage in actions such as creating, transmitting, modifying, revoking, or redeeming Ccoins, they send signed messages to the blockchain, which subsequently authenticates the messages to ensure their legitimacy. Before any Ccoin operation, the functionality of the function caller is checked. Ccoins remain on the blockchain until redemption, and each Ccoin operation triggers a new transaction. These transactions include the Ccoin and a script detailing the call message and resulting activities, facilitating review[12].

**3.3. Workflow.** CcBAC distinguishes itself from other access control models in three main ways. Firstly, it enables fine-grained access control through comprehensive access policies that specify who, what, where, when, and how access is granted. These policies ensure secure access by defining strict procedures to follow, while access permissions are represented as digital assets called Ccoins, stored on the blockchain and managed through secure and atomic operations, akin to cryptocurrency transactions. Secondly, access policy verification occurs within a Trusted Execution Environment (TEE) security zone, providing physical protection for relevant programs and securely collecting environmental evidence to facilitate accurate access decisions and monitor the access process. Lastly, these design elements ensure that CcBAC offers fine-grained and responsible access control with encryption-level security trust, effectively preventing unauthorized access. The workflow of CcBAC can be outlined in the following steps:

Step 1: Send the request Participants send operational requests for Ccoin, including transmission, revocation, update, and redemption.

Step 2&Step 3: Verify that the blockchain verifies the request, including message signature, Ccoin validity, and participant permissions on Ccoin. If it is a redemption request, RACO needs to further verify the environmental data.

Step 4: Access and monitoring. After obtaining access permissions, RACO will access resources and monitor access activities based on policies.

Step 5: Record. Store the accessed records in the blockchain for auditing purposes.

The verification process in CcBAC consists of two main components. Firstly, it verifies identity and transaction authenticity through the blockchain. Secondly, it validates access control policies via the policyCheck function within the authorization process services, which relies on the trusted access control object RACO implemented using Trusted Execution Environment (TEE) technology. Upon receipt of an access request, RACO collects data from the physical environment and securely communicates with the blockchain system to extract access policies from the corresponding Ccoins. To efficiently manage Ccoins within distributed ledgers, the

Table 4.1: Experimental Environment and Configuration

| Configuration | Specific information |
|---|---|
| operating system | Ubuntu 18. 04. 1 GNU/Linux |
| CPU | 8 Intel (R) Core (TM) i7-6700HQ CPU @ 2. 6GHz |
| network card | Intel Corporation Ethernet Connection (2) I219-LM (rev 31) |
| Memory | 16G Samsung PC4-2400T-UA2 |
| Hard disk | 512G SSD Samsung SSD, 1T HDD<br>ST1000DM003-1SB1 CC4 |
| TEE chipset | ARMv8-M TrustZone, LPC55S69-EVK |

UnRedeemed Policy Output (URPO) model, modeled after Bitcoin's Unspent Transaction Output (UTXO) model, has been developed. This model organizes multiple Ccoins within each block, meticulously recording their metadata and transactional activities within the TX script fields. Access policies in Ccoin are represented using JSON key-value pairs, enabling flexible policy granularity. CcBAC inherently incorporates auditability and traceability, as every operation and resource access activity is meticulously logged in the TX script field of transactions stored on the blockchain. This information is openly accessible and serves to provide a comprehensive record of system activities, and validated by the entire blockchain network[13,14].

## 4. Result analysis.

**4.1. Experimental analysis.** The CcBAC system, as proposed by the author, comprises two key components: a blockchain-based distributed ledger and a trusted access control object leveraging TEE chipsets. The blockchain serves as a secure platform for managing Ccoins, facilitating Ccoin operations through transactions, and recording all activities for auditability purposes. Meanwhile, the trusted access control object integrates blockchain clients and sensor drivers within its secure zones, enabling it to gather environmental data and make reliable access control decisions.

In the second component of the system, the experiment employed the LPC55S69-EVK microcontroller in conjunction with sensors including a GPS receiver, temperature sensor, and camera, all safeguarded by ARMv8-M TrustZone. ARMv8-M TrustZone, renowned for its energy-efficient design, consists of a secure zone, a non-secure callable interface, and a non-secure zone. Unlike traditional architectures that isolate non-secure zones from secure resources, TrustZone allows security codes in secure zones to have elevated permissions, enabling access to resources in both secure and non-secure zones. To ensure the secure collection of environmental data essential for access policies, the experiment incorporated a sensor driver within the secure zone of the TEE. This driver facilitates direct communication with sensor hardware. Additionally, a lightweight blockchain client was integrated into the security zone of the TEE, enabling secure communication with the blockchain through SSL/TLS protocols[15]. The experimental setup and configurations are elaborated in detail in Table 4.1.

**4.1.1. Adaptability analysis.** To gauge the versatility of the author's prototype system across various mainstream platforms, the experiment deployed the prototype on three separate platforms: Golang, the Ethereum main network, and the Ethereum-based consortium chain Quorum. Each function within the model underwent independent testing 50 times, and the average runtime for each function on different platforms was recorded. The performance testing of various functions within the Golang prototype revealed relatively uniform time distribution and stable performance. Notably, functions such as createCcoin, transferFrom, updatePolicy, and revokeCcoin demonstrated relatively brief runtimes, spanning from approximately 30 to 80 milliseconds. Conversely, the redeemCcoin function demanded more time due to its involvement in policyCheck. This process entails the sampling and analysis of sensor readings by the access control object of CcBAC, as well as the execution of necessary actions and transmission of data back to the blockchain, thereby resulting in a longer runtime.

Figure 4.1 illustrates the total time duration for each Ccoin operation function across the three prototype systems. Utilizing a logarithmic scale, the figure effectively visualizes the considerable difference in confirmation times between Go Coin and Ethereum Ccoin on various platforms. Upon closer examination, it becomes appar-

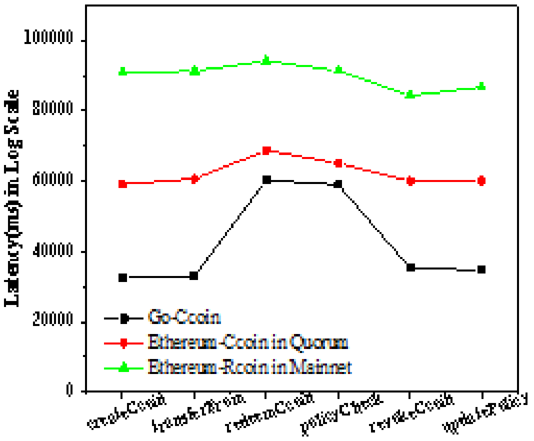

Fig. 4.1: Running Time of Each Function under Three Prototypes

ent that native Go Coins generally require only 40-60 milliseconds to confirm each transaction. In comparison, Ethereum Ccoins within the Quorum consortium chain require approximately 1 second for confirmation, while on the Ethereum main network, this confirmation time extends to approximately 30 to 50 seconds. These findings underscore the good adaptability of the CcBAC model proposed by the author across different platforms.

**4.1.2. Performance analysis.** To assess the performance of the CcBAC system, the experiment utilized the Go Coin prototype and conducted simulations with multi-threaded clients to simulate concurrent access. Two sets of comparative experiments were designed for this purpose. In the first set, the processing time of each function was measured for varying numbers of concurrent requests, ranging from 50 to 1000 virtual clients. The findings, as depicted in Figure 3-4, reveal a consistent pattern. Figure 3 demonstrates that as the number of requests escalates from 50 to 500, the total runtime of each function steadily rises, albeit at a diminishing rate beyond 500 requests. Meanwhile, Figure 4 illustrates a slight increase in the average time cost of functions as the number of requests climbs from 50 to 200. However, with additional requests, there's a subsequent decrease in average time cost, ultimately stabilizing over time[16]. These results suggest that the system's throughput grows as the number of requests increases. Once a certain threshold is reached, throughput stabilizes, with no significant decline observed even as the number of clients continues to rise.

**4.2. Security Analysis.** In real-world scenarios, access control systems are vulnerable to two main types of attacks: access permission forgery and access policy violations. To model the competitive dynamics between honest nodes and attacking nodes, the author employs a binomial stochastic process. This process determines that an attack is successful only if the block length created by the attacking node surpasses the length created by the honest node. If the probability of the attacker ultimately winning the game is p, then both the attacker's victory and failure need to meet certain conditions. Assuming that the probability of the attacker succeeding in each operation is q and the probability of the honest node succeeding in each operation is p, the probability of the attacker winning p can be calculated using the Gambler's Ruin Problem (GRP) formula. Since k may be any integer greater than or equal to 0, the probability of k taking a value follows a Poisson distribution, and the probability of k occurring is equation 4.1:

$$p_k = \frac{\lambda^k e^{-\lambda}}{k!} \tag{4.1}$$

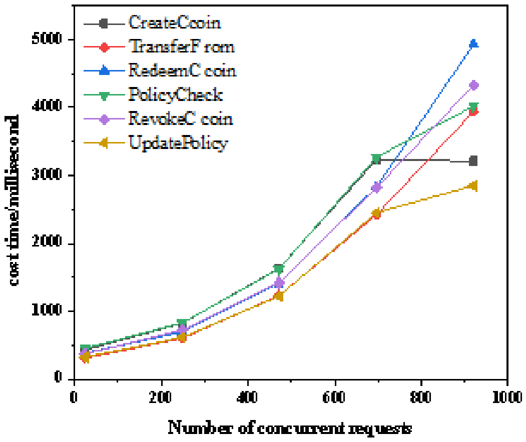

Fig. 4.2: Time cost of functions under different concurrent request quantities

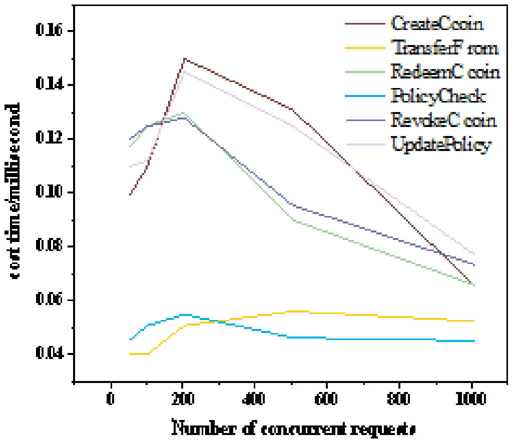

Fig. 4.3: Trend of Average Time Cost of Functions under Different Concurrent Requests

Among them, $\lambda$ is the mean of k, and the ratio relation equation 4.2 below is satisfied:

$$\lambda = z \cdot \frac{q}{p} \tag{4.2}$$

When the tampering chain extends k blocks, the probability of catching up with the honest chain is equation 4.3:

$$q_z = f(x) = \begin{cases} 1, p \leqslant q \\ (\frac{q}{p})^{z-k}, p > q \end{cases} \tag{4.3}$$

Compute the probability of all values from k to positive infinity, then add them up, and finally calculate

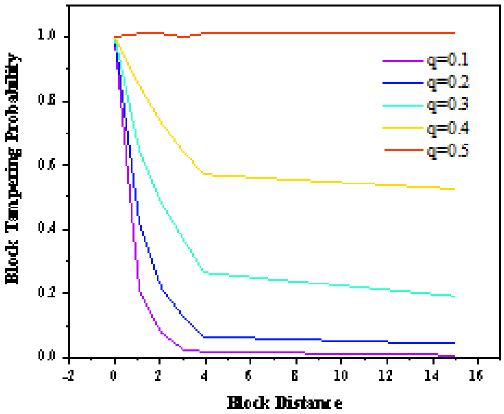

Fig. 4.4: Probability of successful attack

the probability formula 4.4 for attackers to successfully tamper with block data:

$$P=\sum_{k=1}^{\infty}\frac{\lambda^k e^{-\lambda}}{k!}\cdot\begin{cases}(\frac{q}{p})^{z-k}, k\leqslant z\\ 1, k>z\end{cases} \tag{4.4}$$

To avoid infinite sequence summation when calculating the final result, further transform it into equation 4.5:

$$P=1-\sum_{k=1}^{\infty}\frac{\lambda^k e^{-\lambda}}{k!}\cdot(1-(\frac{q}{p})^{(z-k)}) \tag{4.5}$$

The author conducted simulation experiments using MATLAB to analyze the relationship between the probability of block tampering (P) and the number of blocks (n), as illustrated in Figure 4.4. As the number of blocks in the blockchain increases, the probability of successful attacks diminishes rapidly. It becomes evident that attackers require control of more than 50% of the nodes in the blockchain to successfully tamper with the next block. This implies that the blockchain-based IoT device access control mechanism is highly effective in thwarting access permission forgery attacks. Given the vast number of devices in the IoT ecosystem, each capable of serving as a light node in the blockchain, the security of access control is bolstered. Consequently, the author's approach to blockchain-based IoT device access control effectively mitigates forgery attacks on access permissions, aligning with the stringent security requirements of the IoT ecosystem for device access control [17,18].

In addressing the second type of attack, the author considers access policy violations stemming from weak security in IoT devices themselves. Many IoT devices lack robust security measures, making them vulnerable to breaches in code confidentiality and integrity. Attackers exploit these vulnerabilities in lightweight IoT devices to undermine access control security. To mitigate such risks, the author's CcABC model harnesses Trusted Execution Environment (TEE) to deploy reliable access control objects. This strategy establishes a secure enclave for executing code and safeguarding data, guaranteeing privacy and trustworthiness. TEE interfaces with the physical world to establish secure links with the blockchain, extending trust from on-chain to off-chain activities. By securely retrieving access policies from Ccoins stored in the blockchain, the model makes access decisions based on predefined access conditions and rigorously monitors the access process. This ensures that resource visitors adhere strictly to access policies set by the resource owner, effectively thwarting access policy violations. Another significant factor contributing to policy violation attacks is the coarse-grained nature of the access control model itself. Unlike the author's PBAC access control model, which ensures sufficient granularity, other models primarily focus on users rather than resources. For instance, conventional models may inquire, ”Which users are present, and what resources can they access?” This approach typically involves a subject (the entity seeking access), permissions (the actions permitted), and roles (sets of permissions assigned to subjects). In contrast, the author's model delves into, ”What types of users exist, and what actions can they perform within the environment?” Here, the control comprises a principal (the entity seeking access), permissions (the actions permitted), and roles (sets of permissions assigned to the principal). By defining access control policies based on who, what, where, when, and how, the author's model achieves finer granularity, effectively mitigating the risk of access policy violations.

**4.3. Comparative analysis.** The author evaluates the proposed access control model from two perspectives. Firstly, by comparing it with traditional models, the advantages and disadvantages of the CcBAC model are assessed. It's evident that this model offers distinct advantages in handling the complexities of the modern Internet of Things, particularly in scenarios involving massive scale, dynamic environments, and distributed systems.

On the other hand, compared with existing research models, analyze the advantages of the CcBAC model. The access control model described by the author has the following advantages:

Fine-grained CcBAC access control meticulously specifies who, what, where, when, and how—five crucial elements that shape the precision of access control schemes. This approach effectively answers the question of who has permission to perform specific actions, when, and where.

In terms of security, the model conducts all operations related to Ccoin on the blockchain, ensuring that every message is authenticated via a secure signature mechanism. This approach supports trusted storage and guarantees atomic state transitions. Additionally, a dependable access control object, RACO, is responsible for securely retrieving access policies from Ccoins stored on the blockchain. It then makes access decisions based on predefined access conditions and diligently monitors the entire access process.

*Convenient access for users.* Accessing a specific resource is straightforward—all you need is to redeem the corresponding resource using Ccoin. Additionally, audit procedures enable flexible transfer of Ccoin from one holder to another, facilitating dynamic transfer of access permissions.

*Autonomous authorization.* The model ensures that access to resources is solely determined and granted through Ccoin by the resource owner whenever necessary, without any involvement or intervention from third parties accessing the server.

*Auditability.* The author's CcBAC model has native auditability, as all operations and resource access activities through Ccoin are recorded in the TX script fields of transactions stored in the blockchain, and are publicly and validated by the entire blockchain system.

*Access Process Control.* RACO serves as a dependable access control entity, embodying the responsibilities of resource owners. Apart from validating the functionality of Ccoin and ensuring compliance with fine-grained access conditions, RACO actively monitors the entire access process. Through integration with TEE, it guarantees the secure recording of all activities occurring during access, providing comprehensive oversight and security assurance.

**5. Conclusion.** In practical applications, the author's access control model can be widely applied to various devices in the IoT ecosystem. For example, in industrial control systems, the CcBAC model utilizes the decentralized nature of blockchain technology to create unique digital identities for each device, enabling effective authentication and permission management even in the case of a large number of devices. Through smart contracts, permission allocation and revocation between devices can be automated, reducing the complexity and error rate of manual configuration. In industrial automation, the roles of operators and equipment may dynamically change according to production needs. The CcBAC model allows for quick adjustment of access policies through smart contracts to adapt to these changes, ensuring that only authorized operators can access the corresponding devices and data. The CcBAC model utilizes blockchain technology to achieve unified access control policies for cross regional devices, ensuring consistency and security in distributed environments. The immutability of blockchain ensures the integrity of access records, and any unauthorized access attempts will be recorded and traceable. Industrial automation has strict requirements for real-time response, and the CcBAC model reduces transaction confirmation time and improves system response speed through the fast consensus mechanism of blockchain. The Trusted Execution Environment (TEE) provides a secure environment for performing sensitive operations, such as verifying and executing access policies. This ensures that access control policies can be securely executed even in environments where devices may be vulnerable to attacks.

In summary, the blockchain based IoT device access control model can effectively prevent access permission forgery attacks and meet the security requirements of the IoT ecosystem for device access control. When implementing this model, enterprises need to consider the following suggestions for action:

(1) Enhance IoT Device Security: Implementing a trusted execution environment safeguards the confidentiality and integrity of IoT devices, shielding them from potential exploitation by malicious actors.

(2) Flexible formulation of access policies: Based on actual needs, develop fine-grained access policies to ensure that resource visitors strictly adhere to access policies and prevent the occurrence of access policy violations.

(3) Implement unified access control policy standards: Through blockchain storage policies, it facilitates information sharing and supports unified access control policy standards for all parties, improving system scalability and interoperability.

*Future direction.* Focus on implementing Organizational Based Access Control (CcBAC) in specific application scenarios to address specific challenges in this field. This includes exploring how to design and deploy access control policies targeting specific business needs and security threats to ensure the security and availability of the system. Conduct in-depth research on specific needs in different industries or fields, and develop corresponding solutions to meet customer needs and improve overall efficiency and security of the system.

**Acknowledgement.** This work was supported by 2022 science and technology project of State Grid Hubei Electric Power Co., Ltd, ”research and demonstrational application of key technologies of industrial control security proactive defense architecture for novel power systems”(No.52153222001D).

## REFERENCES

[1] Fan, Y., Liu, S., Tan, G., & Qiao, F. (2020). Fine-grained access control based on trusted execution environment. Future Generation Computer Systems, 109, 551-561.

[2] Jiang, W., Li, E., Zhou, W., Yang, Y., & Luo, T. (2023). IoT access control model based on blockchain and trusted execution environment. Processes, 11(3), 723.

[3] Lee, S., Jo, H. J., Choi, W., Kim, H., Park, J. H., & Lee, D. H. (2020). Fine-grained access control-enabled logging method on ARM TrustZone. IEEE Access, 8, 81348-81364.

[4] Zhou, Q., Elbadry, M., Ye, F., & Yang, Y. (2020). Towards fine-grained access control in enterprise-scale Internet-of-Things. IEEE Transactions on Mobile Computing, 20(8), 2701-2714.

[5] Chattaraj, D., Bera, B., Das, A. K., Rodrigues, J. J., & Park, Y. (2021). Designing fine-grained access control for software-defined networks using private blockchain. IEEE Internet of Things Journal, 9(2), 1542-1559.

[6] Atlam, H. F. , Alenezi, A. , Walters, R. J. , Wills, G. B. , & Daniel, J. . Developing an Adaptive Risk-Based Access Control Model for the Internet of Things. IEEE International Conference on Green Computing and Communications;IEEE International Conference on Cyber, Physical and Social Computing;IEEE International Conference on Internet of Things;IEEE International Conference on Smart Data, 15(6), 3485-3498.

[7] Wang, L. , & Yu, Y. . (2023). Access control method of laboratory cloud data based on internet of things technology. Int. J. Auton. Adapt. Commun. Syst., 16, 31-47.

[8] Wang, R. , Wang, X. , Yang, W. , Yuan, S. , & Guan, Z. . (2022). Achieving fine-grained and flexible access control on blockchain-based data sharing for the internet of things. China Communications (English version), 19(6), 22-34.

[9] Liu, X., Wang, H., Zhang, B., & Zhang, B. (2022). An efficient fine-grained data access control system with a bounded service number. Information Sciences, 584, 536-563.

[10] Yu, D., Hsu, R. H., Lee, J., & Lee, S. (2022). EC-SVC: Secure can bus in-vehicle communications with fine-grained access control based on edge computing. IEEE Transactions on Information Forensics and Security, 17, 1388-1403.

[11] Lee, U., & Park, C. (2020). SofTEE: Software-based trusted execution environment for user applications. IEEE access, 8, 121874-121888.

[12] Li, H., Pei, L., Liao, D., Chen, S., Zhang, M., & Xu, D. (2020). FADB: A fine-grained access control scheme for VANET data based on blockchain. IEEE Access, 8, 85190-85203.

[13] Pareek, G., & Purushothama, B. R. (2020). Proxy re-encryption for fine-grained access control: Its applicability, security under stronger notions and performance. Journal of Information Security and Applications, 54, 102543.

[14] Cao, Q., Li, Y., Wu, Z., Miao, Y., & Liu, J. (2020). Privacy-preserving conjunctive keyword search on encrypted data with enhanced fine-grained access control. World Wide Web, 23, 959-989.

[15] Yin, H., Qin, Z., Zhang, J., Deng, H., Li, F., & Li, K. (2020). A fine-grained authorized keyword secure search scheme with efficient search permission update in cloud computing. Journal of Parallel and Distributed Computing, 135, 56-69.

[16] Zhang, W., Liu, S., & Xia, Z. (2022). A distributed privacy-preserving data aggregation scheme for smart grid with fine-grained access control. Journal of Information Security and Applications, 66, 103118.

[17] Zhang, X., Shi, R. H., Guo, W., Wang, P., & Ke, W. (2023). A dual auditing protocol for fine-grained access control in the edge-cloud-based smart home. Computer Networks, 228, 109735.

[18] Oh, H., Nam, K., Jeon, S., Cho, Y., & Paek, Y. (2021). MeetGo: A trusted execution environment for remote applications on FPGA. IEEE Access, 9, 51313-51324.

*Edited by:* Bradha Madhavan
*Special issue on:* High-performance Computing Algorithms for Material Sciences
*Received:* Apr 23, 2024
*Accepted:* Jun 26, 2024