Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.056730

ARTICLE

A Cross-Multi-Domain Trust Assessment Authority Delegation Method Based on Automotive Industry Chain

Binyong Li[1,2,3], Liangming Deng[1,*], Jie Zhang[1] and Xianhui Deng[1]

[1]School of Cybersecurity (Xin Gu Industrial College), Chengdu University of Information Technology, Chengdu, 610225, China

[2]Advanced Cryptography and System Security Key Laboratory of Sichuan Province, Chengdu, 610225, China

[3]SUGON Industrial Control and Security Center, Chengdu, 610225, China

*Corresponding Author: Liangming Deng. Email: 3210810008@stu.cuit.edu.cn

Received: 29 June 2024 Accepted: 12 October 2024 Published: 03 January 2025

ABSTRACT

To solve the challenges of connecting and coordinating multiple platforms in the automotive industry and to enhance collaboration among different participants, this research focuses on addressing the complex supply relationships in the automotive market, improving data sharing and interactions across various platforms, and achieving more detailed integration of data and operations. We propose a trust evaluation permission delegation method based on the automotive industry chain. The proposed method combines smart contracts with trust evaluation mechanisms, dynamically calculating the trust value of users based on the historical behavior of the delegated entity, network environment, and other factors to avoid malicious node attacks during the permission delegation process. We also introduce strict control over the cross-domain permission granting and revocation mechanisms to manage the delegation path, prevent information leakage caused by malicious node interception, and effectively protect data integrity and privacy. Experimental analysis shows that this method meets the real-time requirements of collaborative interaction in the automotive industry chain and provides a feasible solution to permission delegation issues in the automotive industry chain, offering dynamic flexibility in authorization and scalability compared to most existing solutions.

KEYWORDS

Automotive industry chain; cross-domain access; block chain; delegate authority; trust assessment

1 Introduction

The automotive industry chain [1] is an industrial system that covers all aspects of automotive design, research and development, manufacturing, sales, and after-sales service. It consists of several related industries and links, including raw material supply platforms, parts manufacturing platforms, automobile manufacturing platforms, sales platforms, distribution platforms, and after—sales service provision platforms. These links work together to form an interdependent industrial ecosystem to meet the needs of the automotive market. This huge industrial chain provides support for the development and operation of the automotive industry and also promotes the development of related industries and economic growth [2].

Data exchange and collaboration are required between different participants in the automotive industry chain, so trust security between platforms in the multi-domain environment of the automotive industry chain and the security problem of inter-platform data privilege interaction are two obstacles to the development of the automotive industry chain. In order to solve these problems, the automotive industry chain needs to establish a sound access strategy and mechanism. Access control [3–5] is an excellent solution to the security access of platforms in the automotive industry chain. However, with the continuous development of computers, traditional access control models, such as access control lists [6] (ACL), mandatory access control [7] (MAC), role-based access control [8] (RBAC), and attribute-based access control [9] (ABAC), face some challenges. These include single points of failure, low security, low authorization flexibility, and limited dynamic authorization capability.

To solve these issues, this paper proposes a cross-multi-domain trust assessment authority delegation method based on the automotive industry chain. This method combines blockchain technology with trust evaluation mechanisms to provide a dynamic, flexible, and trustworthy solution to the access authorization problem in a multi-domain cooperation environment.

2 Related Work

In contrast to the traditional single static network environment, blockchain-based access control methods [10] in response to the open, complex, multi-change network environment, how to avoid all kinds of cross-domain security risk issues and improve access efficiency and other issues, scholars at home and abroad have carried out relevant research on it. Zyskind et al. [11] in order to satisfy the complex permissions within the enterprise to access and data sharing, put forward an attribute-based encryption access control model, to a certain extent, to solve the problem of difficult to control access rights within the enterprise. Schefer-Wenzl et al. [12] in order to solve the complex automotive industry chain problems, for the automotive production of complex workflow and non-workflow scenarios under the staff to assign reasonable production rights, in order to avoid the problem of manufacturing collaborative work inefficiency. However, the processing capability is limited when the delegated elements are expanded, and due to the diversity and complexity of the supply and demand relationship in the automotive industry chain, the solution cannot meet the needs of all platform users in the industry chain. Aiming at the problems of the authority delegation process, which mainly focuses on the security of the resources of the user body and the low flexibility of authority granting, Wang et al. [13], in order to solve the problem of cross-domain access that cannot be managed at a fine-grained level of authority, trace the path of the authority circulation through the directed hypergraph, divide and combine the coarse-grained tokens, disperse the user power, and realize the business distribution on each domain to satisfy the principle of minimum authorization [14]. Yuan et al. [15] achieved cross-domain access of mobile nodes for cloud environment, role-based access control model, combined with delegation mechanism and quantitative role technology to solve the problem of dynamically changing domains on mobile terminals, and effectively avoided the problem of resource consumption by frequent access of malicious nodes. Zhang et al. [16] proposed a cross-domain access control method based on context-level relationship for the demand of permission management under the business scenarios of the new generation of regulation and control system, which effectively guarantees the security of cross-domain access and facilitates the configuration of cross-domain access constraints by authenticating the permission rules configured by roles based on the contextual relationship of the domains to which they belong. Zhu et al. have developed a discrete conformable fractional grey system model, which provides a novel tool for forecasting and mitigating carbon dioxide emissions related to the automotive sector [17]. This model can be incorporated into trust assessment frameworks to ensure adherence to environmental standards and regulations.

Cai et al. proposed a deep recommendation model by analyzing the cross-grained sentiments between user reviews and ratings [18]. This model can be utilized in the automotive industry for customer feedback analysis, assisting businesses in gaining a better understanding of customer needs and making more informed decisions in the processes of trust assessment and authority delegation.

Trust assessment mechanism [19,20] is an entity's assessment and decision-making of the degree of trust in others in policies and behaviours, which can effectively reduce the complex access control policy formulation. Tian et al. [21] designed a user behaviour trust assessment algorithm for the scenario of complex interactions between users and data in the process of network data access to assess the level of trust in user behaviour during access, and to prevent overstepping access according to the automatic access control technology. Khan et al. [22], aiming at the fact that user privileges are not affected by dynamically changing time factors, integrate the role-based access control model with the blockchain technology and the user credit assessment mechanism, design the credit threshold, and take the credit degree obtained at the end as the basis of whether the role can get the corresponding access privileges. From this, it can be seen that by introducing the trust assessment mechanism and combining multiple judgement factors, the dynamic management of permissions can be achieved, and the access of low integrity entities and no integrity entities to object resources can be prevented to a certain extent. Lin et al. [23], for the access demand in the multi-domain environment of cloud computing, provided a trust-based access control mechanism for cloud computing. Firstly, trust is introduced into the cloud computing environment to establish a trust relationship between users and cloud platforms. This paper also analyses the difference between intra-domain trust and inter-domain trust. In addition, this paper gives the combination of role-based access control framework with multi-domain trust. The access control in this locale directly applies the RBAC model combined with trustworthiness. Zhu et al. [24] proposed a method that uses blockchain technology to enhance the traceability of original achievements, which is important for protecting intellectual property and ensuring supply chain transparency in the automotive industry. Zhu et al. [25] conducted research that sheds light on the complexity of consumer behavior in online flash sales, which can help in designing more effective trust assessment models for automotive consumers' purchasing decisions on e-commerce platforms.

The above research lacks the supervision of honest and legitimate nodes, and how to avoid apparently honest nodes from doing harm also has significant research value. Therefore, a cross-multi-domain trust assessment authority delegation method based on the automotive industry chain is proposed to provide a dynamic, flexible, and trustworthy solution to the access authorization problem under the multi-domain cooperation environment of the automotive industry chain.

3 General Framework Construction

In order to provide work efficiency and quality, the authority of different domains is entrusted to the corresponding departments or units to handle and complete, and the model for solving the multi-domain authorisation problem is shown in Fig. 1.

It mainly contains the following key steps:

(1) Define the different enterprises involved in the industry chain and define the tasks and responsibilities of each domain or enterprise.

(2) Confirm the delegation relationship according to the nature and requirements of each enterprise to ensure the smooth execution of the delegated tasks and the efficient completion of the collaborative work.

(3) Carry out real-time monitoring, and make authorisation adjustments and continuous improvements based on the feedback results.

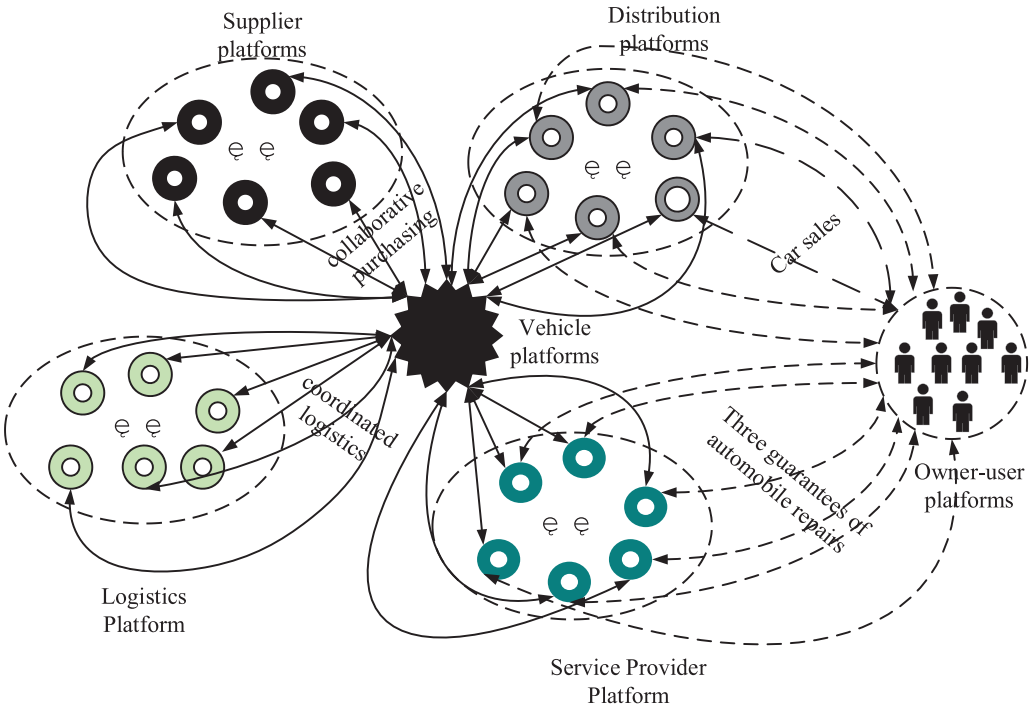

Figure 1: Automotive industry chain service model

The business collaboration in the automotive industry chain mainly consists of four core areas: procurement, sales, after-sales service, and logistics services. These operations need to be coordinated around the vehicle manufacturers and involve information exchange on a cloud service platform. As a result, the collaboration of the four core business areas leads to the formation of four sub-platforms on the cloud service platform. Different vehicle manufacturers establish different information interaction domains for these four sub-platforms on the cloud platform, giving rise to trust evaluation and control issues during cross-domain access.

The proposed method in this chapter combines blockchain and trust assessment, and the architecture is shown in Fig. 2.

It consists of Authorise Domain (AD), Entrusted Domain (ED), Trust Calculation_SC, Network Condition Assessment Point, Historical Behavior Database, Behavioral Recording Database, Trust Renewal_SC, where the Historical Behavior Database, Behavioral Recording Database, Trust Renewal_SC, and Trust Renewal_SC are all in place. Condition Assessment Point, Historical Behavior Database, Behavioral Recording Database, and Trust Renewal_SC, where:

(1) The entrusted party is an entity user, terminal or application that has all or part of the authority of a certain resource in the automotive industry chain enterprises in the multi-domain cooperation environment.

(2) The entrusted party is an entity in the automotive industry chain enterprise in the multi-domain cooperation environment that can obtain the operation privileges that it does not have by accepting the

privileges passed by other users, terminals, applications, etc., so as to achieve the cooperative operation on the chain.

(3) The trust calculation contract is a contract that calculates the trust value of the entrusting party's domain for the permission entrustment request initiated by the entrusting party, and returns the corresponding authorisation decision based on the trust value.

(4) Network Posture Assessment Points (NPAP) provides real-time network change information of the automotive industry chain, and provides the trust calculation contract with the comprehensive assessment value of the network environment in the current multi-domain cooperation environment.

(5) Historical Behavior Database (HBD) is a kind of off-chain database that stores the IP address information used by the client for historical login and the geographic location information used for historical login.

(6) Behavioral Recording Database (BRD) is a kind of off-chain database that stores the historical and current behavioural information of each delegated party domain on the privilege entrustment path, and it can judge and eliminate the evil nodes on the entrustment path through the recorded behavioural information.

(7) The trust update contract is to update the trust evaluation value of the delegator and the delegated party, and the updated evaluation value will be used as the basis for the trust evaluation judgement of the next delegated access.

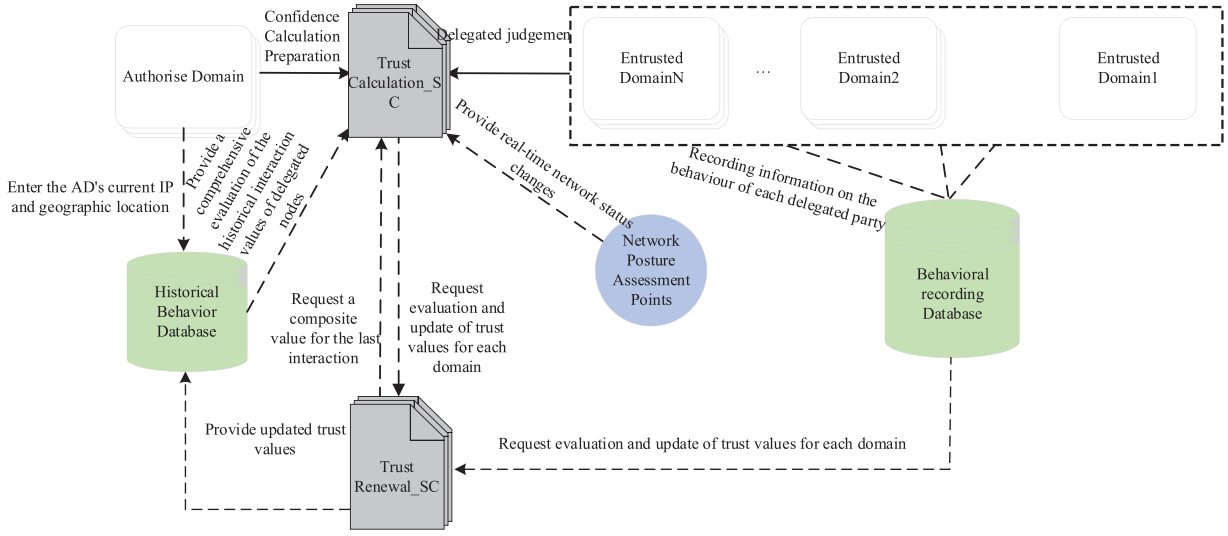

Figure 2: Overall framework model of the proposed methodology

In the following section, the detailed design details of the trust assessment mechanism method, Trust Calculation Contract (Trust Calculation_SC), Trust Renewal Contract (Trust Renewal_SC), and permission granting and retrieval will be elaborated in turn, and the overall operation flow of the overall framework model will be explained.

3.1 Design of a Trust Assessment Mechanism

In the automotive industry chain trust assessment mechanism as used to assess the trust level of each enterprise participant in a multi-domain environment to ensure the security and reliability of access or authority operations, the main design steps are as follows:

(1) Firstly, ensure the dimensions involved in the participants in the trust assessment, which in the automotive industry chain include the participants' identity authentication, behavioural history, and transaction records.

(2) Set the trust level assessment criteria, and develop specific and fine-grained assessment criteria for participants on each different domain.

(3) Establish an assessment method applicable in the automotive industry chain based on the designed dimensions and trust level assessment criteria for assessing and calculating the trust level of participants.

(4) Implement supervision and optimisation strategies, real-time supervision of the assessment results, real-time corresponding assessment strategies, and consideration of comprehensive factors in the chain to ensure that the trust assessment can effectively prevent risky participants and safeguard the privacy and data security of other participants.

3.1.1 Trust Level

In order to facilitate with the automotive industry chain can be based on the participants can be based on their trust results to make the appropriate security measures and operating privileges, the need to establish a trust level hierarchy, this section will be set up for the trust level of the trust level of five levels, including the high warning trustworthy value, warning trustworthy value, pass the trustworthy value, the general trustworthy value, high trustworthy value, the threshold value of the various levels of the design of the Table 1 shows.

Table 1: Table of trust level hierarchy and threshold boundaries

Description of trust	Trust level	Range of values
High warning trust	Trust_Level = 1	[0, 0.3]
Early warning trust	Trust_Level = 2	(0.3, 0.5)
Passing trust	Trust_Level = 3	[0.5, 0.6]
Fair trust	Trust_Level = 4	(0.6, 0.8)
High trust	Trust_Level = 5	[0.8, 1]

According to the actual working situation of the automotive industry chain, the trust assessment judgement formula involved in this section is:

$$\text{Trust\_}Value_i^j = \begin{cases} \dfrac{\sum_{k=1}^{To_i^j} {}^{(k)}\text{Re}_i^j \bullet {}^{(k)}time}{\sum_{k=1}^{To_i^j} {}^{(k)}time}, & To_i^j > To_i^{j'} \\ 0.5, & To_i^j = 0 \\ \delta \bullet NEvalue + (1-\delta) \bullet \dfrac{\sum_{k=1}^{To_i^j} {}^{(k)}\text{Re}_i^j \bullet {}^{(k)}time}{\sum_{k=1}^{To_i^j} {}^{(k)}time}, & 0 < To_i^j < To_i^{j'} \end{cases} \tag{1}$$

where ${}^{(k)}\text{Re}_i^j$ denotes the kth trust assessment record from AD_i to ED_j; To_i^j denotes the total trust assessment value generated between AD_i and ED_j, and $To_i^{j'}$ denotes the total trust assessment threshold between AD_i and ED_j, which is used to avoid malicious, non-honest and other devices obtaining a higher total trust assessment value through fewer honest authorisation operations. When AD_i and ED_j establish the authorisation relationship for the first time, i.e., $To_i^j = 0$, the trust assessment value is set to 0.5 according to the actual situation of multi-domain cooperation environment in the automotive industry chain.

NEvalue is the network environment factor that changes in real time, in this section the network environment factor will be determined by monitoring the geographical location and IP address of the entity logging in, which together determine the network environment factor, which satisfies the following equation:

$$NEvalue = \alpha \cdot \sum_i^j Loction\_value + \beta \cdot \sum_i^j IP\_value \tag{2}$$

where $\alpha \in (0, 1)$, $\beta \in (0, 1)$ and $\alpha + \beta = 1$; *Loction_value* is the evaluation value of the geographical location used by each entity logging in on this delegation path, while *IP_value* is the evaluation value of the IP address used by each entity logging in on this delegation path. The evaluation value distribution of *Loction_value* and *IP_value* is shown in Tables 2 and 3:

Table 2: Assignment of assessed values for logged-in geographic addresses

Abnormal login address	Untrusted and unusual login address	Untrusted and frequent login address	Trusted and infrequent login address	Trusted and frequent login address
[0, 0.2)	[0.2, 0.4)	[0.4, 0.5)	[0.5, 0.8)	1

Table 3: Assignment of evaluation values for logged-in IP addresses

Abnormal login IP address	Untrusted and infrequent login IP address	Untrusted and frequent login IP address	Trusted and infrequent login IP address	Trusted and frequent login IP address
[0, 0.2)	[0.2, 0.4)	[0.4, 0.5)	[0.5, 0.8)	1

${}^{(k)}time$ as a time decay factor, ${}^{(k)}time \in (0,1)$, the expression is:

$$ {}^{(k)}time = \lambda \cdot \frac{time^{end}_{{}^{(k)}\mathrm{Re}_i^j} - time_{first} + 1}{\sum_x^{To_i^j}\left(time^{end}_x - time_{first} + 1\right)} + (1-\lambda)\cdot \frac{time^{end}_{{}^{(k)}\mathrm{Re}_i^j} - time^{start}_{{}^{(k)}\mathrm{Re}_i^j} + 1}{\sum_x^{To_i^j}\left(time^{end}_x - time^{start}_x + 1\right)} \tag{3} $$

where $time_{first}$ denotes the end moment of the authorisation operation of the first trust record of AD; $time^{end}_{{}^{(k)}\mathrm{Re}_i^j}$ denotes the end moment of ${}^{(k)}\mathrm{Re}_i^j$ (i.e., the kth trust assessment operation of AD_i to ED_j); $time^{start}_{{}^{(k)}\mathrm{Re}_i^j}$ denotes the start moment of ${}^{(k)}\mathrm{Re}_i^j$ (i.e., the kth authorisation operation of AD_i to ED_j); $time^{end}_x$ denotes the end moment of the xth trust authorisation of AD_i; $time^{start}_x$ denotes the start moment of the xth trust authorisation of AD_i; λ is the weighting factor and $\lambda \in (0,1)$, and is set according to the actual situation of the multi-domain cooperation environment of the automotive industry chain.

3.1.2 Design of Trust Calculation Contract and Trust Update Contract

The main function of the trust calculation contract is to achieve the calculation of the trust assessment of the entrusted party and to judge whether the authorised unit has the right to collaborate on the operation, aiming to assess and manage the trust relationship between the entities in the automotive industry chain in a dynamic, history-and behaviour-based way. Since the trustworthiness of the delegated party's permission request is the key to determine whether the permission delegation path can be executed safely and credibly, the trust assessment value of all the delegated parties on the delegation path can be calculated and judged to decide whether to carry out the permission delegation operation or not. The main function of the trust update contract is to dynamically update the trust value of each entrusted party after the completion of a privilege entrustment and provide a trust basis for the next privilege entrustment, aiming at realising the dynamic adjustment and updating of the trust relationship between each entity in the automotive industry chain in a history-based way. This process is based on the latest behaviour of the entities, changes in the network environment and other factors to update the trust relationship in a comprehensive manner, adjusting the trust relationship in a timely manner according to the real-time data and dynamic changes in the environment to ensure the accuracy and effectiveness of the trust relationship, see Algorithms 1 and 2.

Algorithm 1: Trust Calculation_SC

Input: $Request_{AD}$, *Loction_value*, *IP_value*
Output: Boolean

```
1.   Get  Trust_Value Form Trust Renewal_SC  then
2.   Judge(Trust_Value);
3.   if  (Trust_Value ≤ 0.3?) then
4.      Delegate Denied;
5.      Return false;
6.   else
7.       for i to j Get Loction_value && IP_value  from NAPA &&
8.       Get Historical composite assessment value from HBD  then
9.       Calculate(Loction_value && IP_value &&Historical composite assessment value)
          →New_Trust_Value;
10.      if  (New_Trust_Value ≤ Minimun_trust  assessment value)  then
11.         Delegate Denied;
12.         return  false;
```

(Continued)

Algorithm 1 (continued)

```
13.          else
14.              Send New_Trust_Value to Trust Renewal_SC;
15.              return true;
16.          end if
17.      end if
```

Algorithm 2: Trust Renewal_SC

```
Input: New_Trust_value
Output: Boolean
1.      Get New_Trust_value Form Trust Calculation_SC then
2.      Calculate(New_Trust_value && Historical_Trust_value)→Total_Trust_value;
3.      if (0.6 ≥ Total_Trust_value ≥ Minimun_trust assessment value?)then
4.          Update(Trust_Level = 3, Total_Trust_value)→HBD;
5.      else if (0.8 ≥ Total_Trust_value ≥ 0.6)
6.          Update(Trust_Level = 4, Total_Trust_value)→HBD;
7.      else if (Total_Trust_value ≥ 0.8)
8.          Update(Trust_Level = 5, Total_Trust_value)→HBD;
9.      else
10.         return false;
11.     end if
12.     return true;
```

Combined with the overall framework model of the proposed method in Fig. 2 and the details of the algorithm, the overall operation flow of the multi-domain delegated authority control method is as follows:

Step1: When the delegator initiates the delegate request, firstly the delegator will evaluate the historical trust of all the delegated nodes on the delegate path, and will obtain the historical trust evaluation value of each delegated node from the trust update contract, when $Trust\_Value \leq 0.3$ indicates that the delegated node has dishonest operation in history, then the delegator will reject the delegated authority request, and return the result; otherwise, go to Step2.

Step2: Trust computing contract will obtain the geographic login location and IP address of each delegated node from NAPA, and calculate the corresponding *Location_value* and *IP_value*, and also obtain the historical interaction comprehensive evaluation value of each delegated node from HBA, and calculate the value based on their respective weights; and then go to Step3.

Step3: the trust calculation contract will evaluate the latest obtained value *New_Trust_Value*, when it is less than the minimum trust evaluation value, the delegator rejects the privilege delegation request and returns the result; otherwise, the *New_Trust_Value* will be returned to the trust update contract, and jump to Step4.

Step4: After receiving the authorization request *New_Trust_Value* from the trust calculation contract, the trust update contract will weight the trust evaluation value of the delegated node and the historical trust evaluation value according to their respective weights, and based on the result obtained *Total_Trust_value*, update the trust level of the delegated node and return the result to the historical behaviour database, which will be used as the basis for the next privilege delegation.

3.2 Delegated Trust Evaluation Based on Blockchain

The core of the method proposed in this paper is to use blockchain technology for delegated trust evaluation and permission granting. To clearly explain the entity receiving the authorization and how blockchain is used to achieve the set objectives, Fig. 3 presents a diagram of the delegated trust evaluation mechanism based on blockchain.

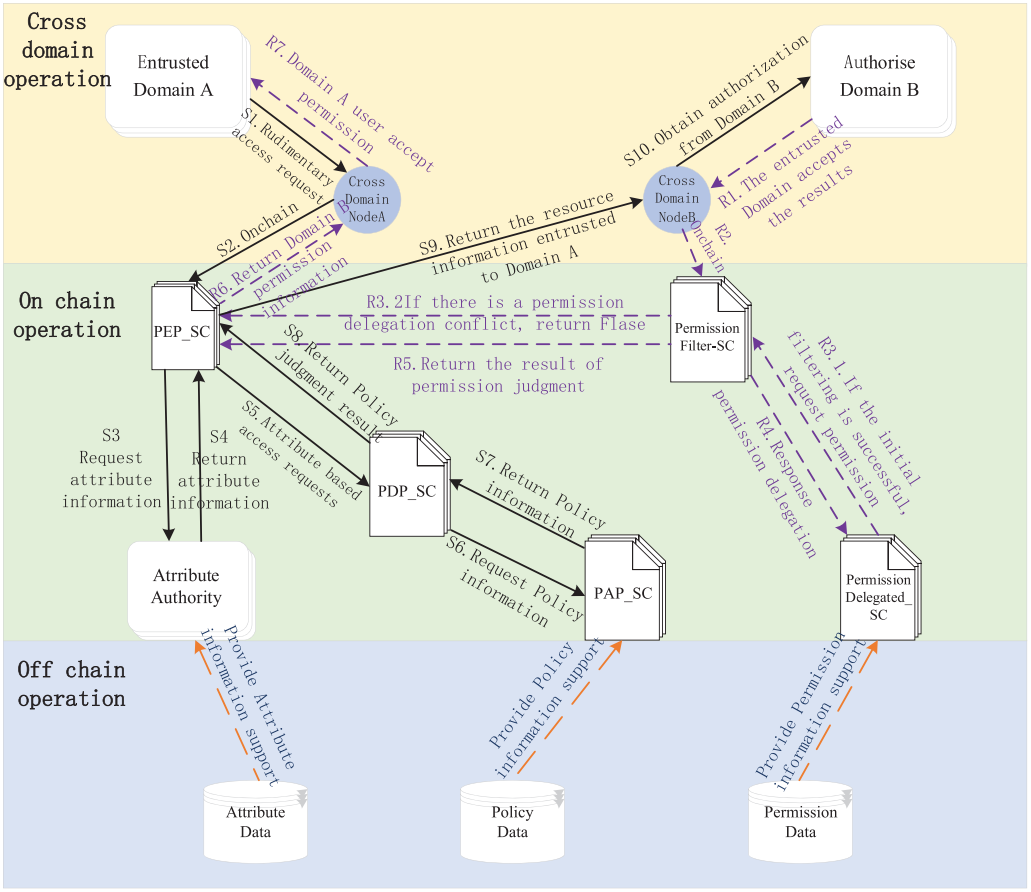

Figure 3: Blockchain operation mechanism design

To achieve cross-platform information sharing, the main blockchain defines smart contracts for the operational rules of each platform. The table shown as Table 4 explains the five involved smart contracts one by one to facilitate access and integration across multiple platforms.

For the sub-blockchain that records activity and attribute data, policy data, and permission data, this paper uses off-chain operations with a MySQL database to store activity logs and information data. For off-chain data containing sensitive information, encryption is applied, and only authorized users with a unique security identifier can decrypt and access the data. The inter-domain access control mechanism is implemented based on the Hyperledger Fabric blockchain platform, and performance tests are conducted. In Hyperledger Fabric, the consensus mechanism is flexible, allowing participants to choose a suitable consensus algorithm based on business needs. For the automotive industry chain's multi-domain environment, considering the network scale, performance requirements, and security needs, this paper chooses the Kafka consensus algorithm. Kafka uses distributed logs to achieve

consensus by sending transactions to a Kafka channel, where multiple subscribers can order and replicate transactions, ensuring data consistency and reliability while preventing tampering and errors. This mechanism achieves high throughput and fault tolerance to meet the demands of the automotive industry chain.

Table 4: Smart contract definition and description

Smart contract name	Description
PEP-SC (Policy Enforcement Point Smart Contract)	Responsible for receiving original access requests from user nodes on a domain, forwarding requests to the Attribute Authority to get attribute information. After PDP evaluation, it determines whether the user has access to information on other domains.
PAP-SC (Policy Administration Point Smart Contract)	Responsible for initializing and formulating policy information and providing it to PDP for decision-making.
PDP-SC (Policy Decision Point Smart Contract)	Retrieves policy information from PAP, evaluates attribute-based access requests, and makes decisions based on the policy set.
Permission Filter-SC (Permission Filter Smart Contract)	Dynamically filters to prevent authorization conflicts by checking if the delegated node belongs to the access control matrix and if its trust level meets the minimum threshold. It returns a filtered authorization result.
Permission Delegated-SC (Permission Delegated Smart Contract)	If the request passes through the permission filter-SC, the contract retrieves the appropriate permission from the permission database using the delegator's ID and returns the result.

As shown in Fig. 3, we can see that in the cross-domain operation module, Domain A is the delegated entity that receives the authorization. The way to obtain the permissions is through Domain A gaining access rights to Domain B via the access control mechanism. Domain B users realize the delegation of permissions between the delegator and the delegatee through cross-domain nodes. The blockchain operates as shown in the on-chain operation module in Fig. 3, where the access method combines the ABAC model with blockchain technology. The various function execution points of the ABAC model (PEP, PDP, PAP) are implemented as smart contracts to ensure decentralization and transparency during the access control process. In the authorization module of the on-chain operation module, the delegatee must pass through permission filtering and granting design, ensuring that cross-domain delegation is only performed when there is no conflict in permission granting. This ensures the

reliability and security of the permission delegation, enabling collaborative utilization of cross-domain resources and enhancing the efficiency and competitiveness of the entire industry chain.

3.3 Permission Granting Management across Multiple Domains

To prevent the risk of information monopolies arising from excessive authority delegation within the automotive industry chain, it is imperative that the business allocation across each domain adheres to the principle of separation of duties. In light of this, this section introduces a Multi-Domain Delegated Management Mechanism (MDDM), which is implemented on nodes that span multiple domains. When the 'Times' parameter, which denotes the permissible number of passes, exceeds one, the mechanism is activated. This activation ensures that the cross-domain node scrutinizes the legality of the path from the preceding cross-domain node and the completeness and security of the data, based on the information provided by the previous node in a benign context. Should any alterations to the path be detected, the delivery process is immediately halted, thereby effectively mitigating the risk of malicious nodes tampering with the authorization delivery process.

The 'Date,' 'Times,' 'Depth,' and 'Path' parameters are meticulously configured to rigorously govern the delegation path, thereby circumventing the potential for information leakage due to interception by malicious nodes along the delegation route. Notably, Algorithm 3 is designed to facilitate secure and dependable cross-domain requests and delegations within the multi-domain trading environment of the automotive industry. It safeguards the integrity and privacy of data and ensures the efficient management and restoration of permissions.

This refined approach not only fortifies the system against unauthorized access but also enhances the overall robustness and reliability of the cross-domain management within the automotive industry chain.

Algorithm 3: Multi-domain delegated management mechanism

```
for i = 1 to N do
if (from_userx to D^LP_Order_x is a legal Path)&&(Data < Tertime∩Times = N−1) then
    for i = 1 to N do;
    Send P_fromx0 to next D_Orderx;Times—;
    return true;
    if
        (Date = =Tertime‖Times = =0) then
        RevokePermission(D^LP_Order_x to Userx);
        when
            D^LP_Order_x need active revoke permissions;
            then Set Tertime = =CurrentTime && Permission_Set.buffer/PermissionData
            .Plegal
            Re-authenticate(userx to D^LP_Order_x);
            if
                (userx can't access to D^LP_Order_x)
                return true;
            end if
        end when
    end if
else
```

(Continued)

Algorithm 3 (continued)

```
20.        return false;
21.    end if
```

MDDM algorithm process description:

(1) Traverse the process from the initial state to the end state whether there is a legal path;

(2) Determine whether the authorisation is within the specified time and whether the maximum number of authorisations has been reached;

(3) If the authorisation is within the legal authorisation, then the authorisation will be passed between the two adjacent nodes, and the number of allowed passes will be reduced gradually, otherwise it will return false;

(4) By the deadline time or the allowable number of passes is equal to 0 (when Times is less than 0, it means that there is a malicious node involved in the process of passing permissions), recover the set of permissions issued from the delegated domain;

(5) When it is necessary to actively recover the permissions, change the deadline time to the current time and remove the legitimate authorisation set in the buffer of the permissions set, and verify that the authorisation link between the two is broken by re-authentication, otherwise return false.

4 Experimentation and Analysis of Multi-Domain Delegated Authority Control Methods

In this section, a total of two sets of experiments are designed, namely, the experiment on the effectiveness of the trust assessment mechanism processing of the multi-domain delegated authority control method and the experiment on the efficiency of the method's time-consuming processing, which will be analysed in detail in the next section.

4.1 Experimental Environment Setting

The experiments in this chapter were conducted on an Intel 11th Gen Intel(R) Core(TM) i7-11800H@ 2.30 Hz octa-core processor with 16 GB of RAM and a 64-bit Windows 10 operating system on an open source data "soc-sign-bitcoinalpha", which is a dataset used to study social networks and trust relationships. bitcoinalpha", a dataset used to study social networks and trust relationships, each data point contains an initiator and a receiver, and a trust value between −10 and 10, with −10 indicating the lowest trust level and 10 indicating the highest trust level, to build a model to predict unknown trust relationships between users, thus helping to identify potential frauds. relationships, thus helping to identify potential fraud and build a sound trust assessment system. The basic information and format of the data in "soc-sign-bitcoinalpha" is shown in Table 5.

Table 5: Basic data information and format of "soc-sign-bitcoinalpha"

Data item	Descriptions
SOURCE	Node ID of the source
TARGET	Node ID of the target

(Continued)

Table 5 (continued)

Data item	Descriptions
RATING	Source-to-target rating in the range [–10, 10] in steps of 1
TIME	Rating time

The original data of "soc-sign-bitcoinalpha" has RATING ratings in the range of [–10, 10], and in order to better apply the cross-multi-domain privilege delegation method proposed in this section, the dataset will be preprocessed to normalise the range of RATING values to [0, 1].

4.2 Trust Assessment Experiment

(1) Experiment on processing the effectiveness of trust assessment mechanism for multi-domain delegated authority control methods

In this experiment, different delegated subjects initiate authorisation requests to all nodes on the delegated path under the same conditions to verify the change of their trust values. Six different subjects are used for this experiment, including AD1, AD32, AD77, AD129 from the dataset "soc-sign-bitcoinalpha" and the simulated data AD100 and AD200. The parameters of the subjects are set as shown in Table 6.

Table 6: AD parameter settings

AD	Initialize Trust_Level	Initialize *Trust_Value*
AD1	4	0.62314
AD32	3	0.59423
AD77	4	0.61325
AD129	4	0.60362
AD100	2	0.44292
AD200	3	0.58337

This experiment firstly initiated 50 times of authority entrustment requests to different entrusted subjects, in which the first 49 times are legal authorisation entrustment requests and the last time is illegal entrustment request initiated by the entrusted subject, the experimental results are shown in Fig. 4, through the change of *Trust_Value* which it can be seen that there exists the entrusted node because of the number of authority entrustment requests of the previous period is too low leading to the presentation of *Trust_Value* a substantial increase or decrease in the change, but with the number of entrustment requests However, as the number of entrustment requests continues to rise, *Trust_Value* is a slow or relatively stable trend, but when the entrusted subject initiates an illegal entrustment request (i.e., the 50th privilege entrustment request), *Trust_Value* will be a significant drop, and the trust value will directly drop to below 0.3, and its trust level will be graded as Trust_Level = 1, so this kind of entrusted subject will not be able to initiate a request for entrusted operation again, which indicates that the methods involved in this chapter are suitable for identifying and processing illegal privilege entrustment requests. This demonstrates that the methods in this chapter have a good ability to identify and deal with illegal privilege delegation operations.

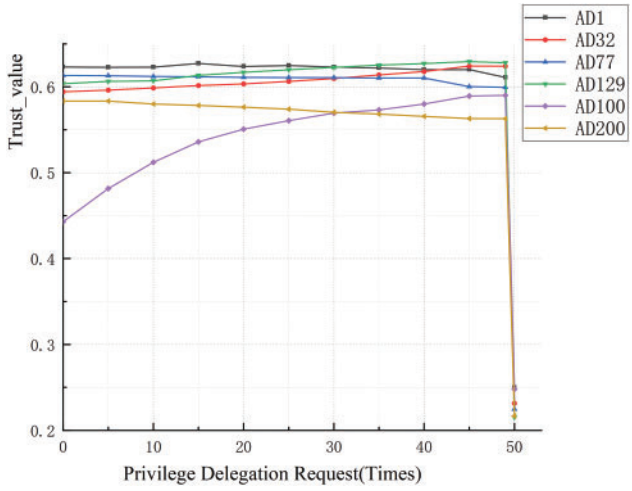

Figure 4: Impact of the number of permission delegation requests on the change of trust assessment value

Secondly, 50 requests for authority entrustment were initiated to different entrusted subjects, and one suspected illegal entrustment request was initiated every 10 entrustment requests, and the experimental results are shown in Fig. 5, which shows that with a large number of legal authority entrustment requests, the overall change of *Trust_Value* shows a trend of gradual stabilization, but whenever there is a suspected illegal request for authority entrustment, the *Trust_Value* will be reduced in a small amount, and because the information obtained by each request will provide the basis for the next trust evaluation, it will have an impact on each subsequent request, making it difficult to change; each time after a suspected illegal request for authority entrustment, it will be difficult to change; each time after a suspected illegal request for authority entrustment, it will be difficult to change. And because the *Trust_Value* obtained from each entrustment request will provide the basis of judgement for the next *Trust_Value*, therefore, after the first occurrence of suspected unlawful entrustment request, it will have an impact on each subsequent, making it difficult to obtain a stable; after each suspected unlawful entrustment request, it is necessary to pass the next lawful entrustment request *Trust_Value* to get a small increase, and with the increasing number of suspected unlawful entrustment requests, this situation is more and more obvious. As the number of suspected illegal requests increases, this situation becomes more and more obvious, so the number of suspected illegal requests has a greater impact on the *Trust_Value*.

(2) Experiment on the time-consuming processing efficiency of the trust assessment mechanism of the multi-domain delegated authority control method

This experiment verifies the processing efficiency of the trust assessment mechanism by calculating the time overhead spent by the trust assessment mechanism in the process of authorisation requests initiated by different delegated subjects. First of all, this experiment prepares 100 delegate nodes, and each node only accepts a delegate request once, and every 4 delegate nodes are passed through a time overhead record. Due to the effect of experimental equipment, there is a certain uncertainty, so the simulated 20 rounds of experimental results to take the middle of the process, the experimental results are shown in Fig. 6.

Through Fig. 6, it can be seen that with the increasing number of delegated nodes, the time overhead spent in the trust mechanism stage also increases gradually, in the 0–12 interval, the time

overhead is extremely low can be ignored, in the 68–80 interval of each delegated node trust assessment time overhead rises sharply. Overall, the average time overhead in completing the processing of authorisation operations for 100 delegated nodes is 4.2016 s, and the trust assessment method is applied in a complex multi-domain co-operative environment, for a large number of delegated nodes, the time required for the trust assessment method is acceptable.

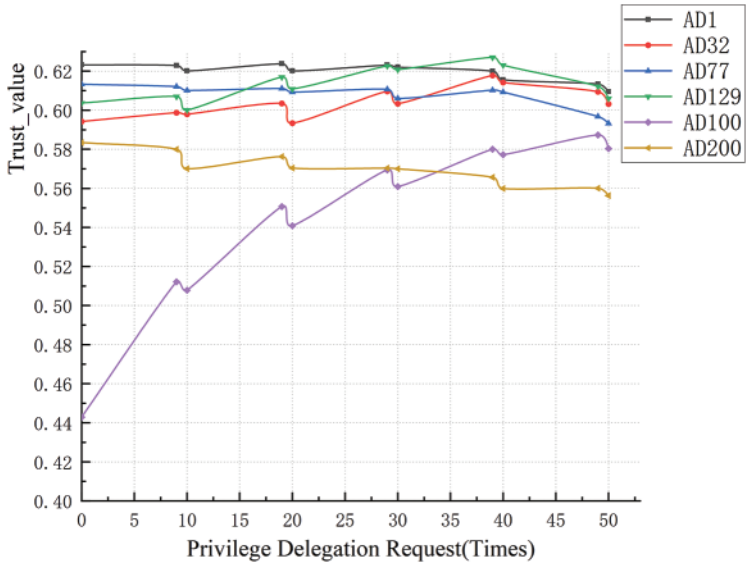

Figure 5: Impact of suspected illegal requests on the change of trust assessment value

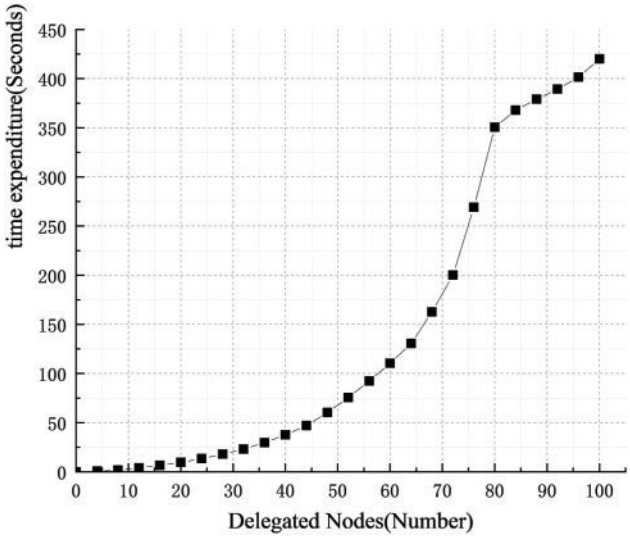

Figure 6: Record of time overhead of the proposed method

4.3 Performance Test Experiment

System performance testing is done to determine the behaviour and response of the system under various expected load conditions. In order to test the concurrency performance of the system, this

experiment will be conducted using 50, 100, 200, 400, 700, and 1000 number of clients for concurrency testing while monitoring and recording the performance metrics as shown in Fig. 7.

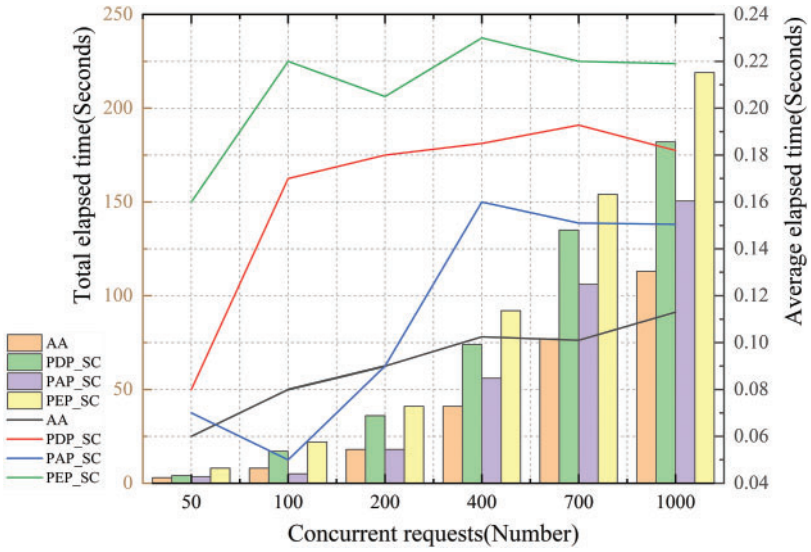

Figure 7: Access policy contract performance test

Fig. 7 shows that the time consumed by the policy execution operation is higher than that of the attribute authority, policy decision, and policy management contracts, and with the rise of concurrency, the total cost of time consumed by each contract module is increased, but the average time consumed is slightly fluctuating and then tends to a stable state. Therefore, for the access policy contract is not affected by the rise of concurrency, resulting in a significant decline in throughput. Moreover, the scheme provided in this paper for user access management only for the first time Wei authentication or long time not logged in the user ABAC fine-grained access control management, the actual frequency of the contract is not high, enough to support the automotive industry chain multi-domain cooperation environment of distributed high concurrent access needs.

5 Conclusions and Outlook

This paper takes the automotive industry chain authority entrustment business as the research background. To address the challenges of cross-domain interactions and the difficulties in establishing authority delegation, it combines blockchain technology, trust assessment, and authority delegation mechanisms. A cross-multi-domain trust evaluation and authority delegation method based on the automotive industry chain is proposed. This method utilizes blockchain technology and a trust assessment mechanism, implemented through smart contracts, to ensure decentralized and transparent access control. The trust level of each participant is evaluated through a set of trust assessment standards, and trust values are calculated based on the participant's geographic location, IP addresses, and historical behavioral records. Experimental results demonstrate that the proposed method is effective, time-efficient, and offers enhanced stability and security compared to traditional privilege delegation schemes.

5.1 Limitations

While the proposed method demonstrates effectiveness in handling cross-domain trust evaluation and permission delegation, several limitations exist. First, the current scheme focuses primarily on trust evaluation and permission delegation without incorporating more complex access control scenarios, such as those involving dynamic reward and punishment mechanisms. This limits the flexibility of the model in adapting to real-world environments where incentives and penalties play a role in access decisions.

Second, the model does not yet account for game theory-based strategies that could optimize decision-making in environments with multiple stakeholders. Such strategies could improve the overall efficiency of permission delegation and access control processes, especially in competitive or cooperative multi-domain settings.

Lastly, although the method has shown promise, further testing in a wider range of application scenarios is necessary to fully assess its adaptability and scalability across different industries and use cases.

5.2 Future Work

Future work will extend the proposed scheme to more access control scenarios, such as reward and punishment mechanisms for access control based on game theory. This extension will enhance the applicability and flexibility of the model, making it suitable for a broader range of real-world application scenarios. Additionally, future studies will explore the integration of game theory-based strategies to optimize decision-making and improve the efficiency of permission delegation processes, particularly in environments with multiple stakeholders.

Acknowledgement: We thank our families and colleagues who provided us with moral support.

Funding Statement: This research was funded by the Sichuan Science and Technology Program, Grant Nos. 2024NSFSC0515, 2024ZHCG0182 and MZGC20230013.

Author Contributions: The authors confirm contribution to the paper as follows: Study conception and design: Binyong Li, Liangming Deng; analysis and interpretation of results: Liangming Deng, Binyong Li; draft manuscript preparation: Jie Zhang, Binyong Li, Liangming Deng, Xianhui Deng. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The authors confirm that the data supporting the findings of this study are available within the article.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

[1] B. Y. Li *et al.*, "Cloud service platform information support system for automotive industry chain," *Comput.-Integ. Manufact. Sys.*, vol. 21, no. 10, pp. 2787–2797, 2015.

[2] X. Yuan, X. Liu, and J. Zuo, "The development of new energy vehicles for a sustainable future: A review," *Renew. Sustain. Energy Revi.*, vol. 42, no. 1, pp. 298–305, 2015. doi: 10.1016/j.rser.2014.10.016.

[3] T. H. Yuen, J. K. Liu, M. H. Au, X. Huang, W. Susilo and J. Zhou, "k-Times attribute-based anonymous access control for cloud computing," *IEEE Transact. Comput.*, vol. 64, no. 9, p. 1, 2014. doi: 10.1109/TC.2014.2366741.
[4] S. Uppuluri and G. Lakshmeeswari, "Secure user authentication and key agreement scheme for IoT device access control based smart home communications," *Wirel. Netw.*, vol. 29, no. 3, pp. 1333–1354, 2023.
[5] H. Liu, D. Han, and D. Li, "Fabric-IoT: A blockchain-based access control system in IoT," *IEEE Access*, vol. 8, pp. 18207–18218, 2020. doi: 10.1109/ACCESS.2020.2968492.
[6] S. Suman and A. Agrawal, "IP traffic management with access control list using cisco packet tracer," 2016.
[7] S. B. Lee *et al.*, "A design of MAC model based on the separation of duties and data coloring: DSDC-MAC," *J. Comput. Sci.*, vol. 16, pp. 72–91, 2020. doi: 10.3844/jcssp.2020.72.91.
[8] J. A. Khan, "Role-based access control (RBAC) and attribute-based access control (ABAC)," in *Improv. Secur., Priv. Trust Cloud Comput. IGI Global*, 2024, pp. 113–126.
[9] E. Yuan and J. Tong, "Attributed based access control (ABAC) for web services," *IEEE*, 2005. doi: 10.1109/ICWS.2005.25.
[10] M. I. H. Ninggal, "Blockchain-based access control scheme for secure shared personal health records over decentralised storage," *Sensors*, vol. 21, 2021. doi: 10.3390/s21072462.
[11] G. Zyskind *et al.*, "Decentralizing privacy: Using blockchain to protect personal data," in *IEEE Secur. Priv. Workshops*, IEEE, 2015. doi: 10.1109/SPW.2015.27.
[12] Schefer-Wenzl, Sigrid, M. Strembeck, and A. Baumgrass, "An approach for consistent delegation in process-aware information systems," in *Int. Conf. Business Inform. Syst. (BIS)*, Berlin, Heidelberg, Springer, 2012.
[13] X. Wang, and S. S. M. Chow, "Cross-domain access control encryption: arbitrary-policy, constant-size, efficient," in *IEEE Symp. Secur. Priv.*, IEEE, 2021. doi: 10.1109/SP40001.2021.00023.
[14] H. Hu and Z. Guo, "The application of cross-domain single sign-on in municipal portal," *IEEE*, 2013. doi: 10.1109/TENCON.2013.6718522.
[15] J. B. Yuan, L. L. Wei, and Q. H. Zeng, "A cross-domain access delegation model for cloud computing for mobile terminals," *J. Softw.*, vol. 24, no. 3, pp. 564–574, 2013.
[16] H. Zhang, J. Wang, and J. Chang, "A multi-level security access control framework for cross-domain networks," in *IEEE Int. Conf. Comput. Sci. Eng.*, IEEE, 2017. doi: 10.1109/CSE-EUC.2017.244.
[17] P. Zhu, H. Zhang, Y. Shi, W. Xie, M. Pang and Y. Shi, "A novel discrete conformable fractional grey system model for forecasting carbon dioxide emissions," *Environ., Develop. Sustain.*, pp. 1–29, 2024. doi: 10.1007/s10668-024-04479-8.
[18] Y. Cai, W. Ke, E. Cui, and F. Yu, "A deep recommendation model of cross-grained sentiments of user reviews and ratings," *Inform. Process. Manag.*, vol. 59, no. 2, 2022, Art. no. 102842. doi: 10.1016/j.ipm.2021.102842.
[19] D. Christin, D. R. Pons-Sorolla, M. Hollick, and S. S. Kanhere, "TrustMeter: A trust assessment scheme for collaborative privacy mechanisms in participatory sensing applications," *IEEE*, 2014. doi: 10.1109/ISSNIP.2014.6827614.
[20] P. S. Pol and V. K. Pachghare, "A review on trust-based resource allocation in cloud environment: Issues toward collaborative cloud," *Int. J. Semant. Comput.*, 2023. doi: 10.1142/S1793351X22400141.
[21] L. Tian *et al.*, "A kind of quantitative evaluation of user behaviour trust using AHP," in *Computat. Inform. Syst.*, 2007.
[22] M. A. Khan, Shalu, Q. N. Naveed, A. Lasisi, S. Kaushik, and S. Kumar, "A multi-layered assessment system for trustworthiness enhancement and reliability for industrial wireless sensor networks," *Wirel. Pers. Commun.*, vol. 137, no. 4, pp. 1997–2036, 2024. doi: 10.1007/s11277-024-11391-x.
[23] G. Lin, Y. Bie, and M. Lei, "Trust based access control policy in multi-domain of cloud computing," *J. Comput.*, vol. 8, no. 5, 2013. doi: 10.4304/jcp.8.5.1357-1365.

[24] P. Zhu, J. Hu, X. Li, and Q. Zhu, "Using blockchain technology to enhance the traceability of original achievements," *IEEE Trans. Eng. Manag.*, vol. 70, no. 5, pp. 1693–1707, 2021. doi: 10.1109/TEM.2021.3066090.

[25] P. Zhu, C. Miao, Z. Wang, and X. Li, "Informational cascade, regulatory focus and purchase intention in online flash shopping," *Electron. Commer. Res. Appl.*, vol. 62, 2023, Art. no. 101343. doi: 10.1016/j.elerap.2023.101343.