Journal of Artificial Intelligence Practice (2025)
Clausius Scientific Press, Canada

DOI: 10.23977/jaip.2025.080204
ISSN 2371-8412 Vol. 8 Num. 2

Adaptive Access Control Model Based on Activity and Trust in Social Internet of Things

Jian Liu[1,a], Lingkang Kong[1], Huihui Yang[1,a,*], Yingchao Wang[1]

[1]Xinjiang College of Science and Technology, Korla, 841000, China
[a]liujian_neulinx@foxmail.com
**Corresponding author*

Keywords: Social Internet of Things; Trust; Activity; Access control; Bayesian authorization; Fine-grained

Abstract: In the process of secure interaction in the Social Internet of Things (SIoT), there is a lack of dynamic flexibility in user trust and insufficient authorization accuracy. This paper proposes an access control model based on SIoT activity and trust (SA-TBAC).The model introduces social relations for SIoT trust evaluation and adaptive weight function to dynamically adjust user trust. Bayesian decision theory is introduced in the authorization decision process, and the object authorization process is regarded as a binary classification problem for the selection of execution decision results. An access control model combining SIoT trust and user behavior trust is established. The experimental results show that the dynamic adjustment of user trust in the interaction cycle increases the accuracy and flexibility of model authorization, improves the success rate of interaction in the cycle, and optimizes the interaction environment compared with other access control models in SIoT.

1. Introduction

The rapid development of Internet technology provides great opportunities for the Internet of Things based on social networks. The Social Internet of Things (SIoT) [1] is a combination of social networks and the Internet of Things, which integrates the characteristics of social networks and the Internet of Things [2]. And gradually applied to new research fields, such as smart home [3-5], smart medical [6-7], smart transportation [8-10] and so on. With the advancement of social networking applications, the security issues it faces are becoming increasingly prominent. Attacks related to the Internet of Things have emerged in an endless stream in recent years. Device security vulnerabilities in the field of smart medical care may even have a serious impact on people's lives. Therefore, it is of practical importance to explore efficient solutions to improve the security of access control such as resource request and permission grant, and to strengthen the security application of social networking[11].

Trust in the Social Internet of Things represents the reliability of the services provided by smart devices. Smart objects build relationships with objects they trust and provide the services they need to people and devices who have established good relationships with them. In order to enable users to obtain more satisfactory services, improve the level of cooperation between intelligent objects, and ensure the security and navigation of the overall network, it is necessary to conduct trust evaluation on social networks. In order to improve the security of legitimate node interaction in the social Internet of Things environment, it is particularly important to select a reasonable access control model to protect resources and data from the theft and destruction of malicious nodes.

2. Related work

There are relatively few studies focused on the combination of SIoT and access control in the existing literature. Authorization decision-making is one of the most critical processes in the access control mechanism. It studied the trust model based on certificate authorization in SIoT and performed trust-based access control through role mapping in [12]. Chang et al.[13] based on trust in the Internet of Vehicles, the authorization strategy is formulated by setting a reasonable threshold, and the flexibility and precision of the authorization decision are insufficient. Zhang et al.[14] implemented an adaptive access control model through game theory and label technology. However, the method of pregranting permissions reduces the security of the entire model. Deng et al. [15] combines dynamic trust evaluation with traditional RBAC model, and authorization decision is still determined by trust threshold. Qiao et al.[16] authorizes based on roles, establishing a mapping relationship between roles and permissions, which enhances the flexibility and accuracy of authorization but slightly compromises security. Liu et al.[17] proposes a new model called TRBAC, which authorizes based on trust levels, thereby strengthening model security at the cost of dynamic flexibility in authorization. In the investigation of the cloud environment, Li and Gong [18-20] focused on the calculation or evaluation of trust, and obtained the degree of trust directly by aggregating trust, while ignoring the dynamic adjustment of trust. Pan and Zhang [21-22] introduced the reward and punishment mechanism and the weight analysis method to realize the dynamic evaluation of trust, but the trust weight factor does not have dynamic adaptability, and the precision of authorization decision making is relatively insufficient. In the cloud environment and the Internet of Things, Subramanian and Oliveira [23-24] has established a trust-based access control mechanism, but the decision accuracy and dynamicity are insufficient.

Based on the existing research, this paper combines the advantages of trust dynamic evaluation and Bayesian decision theory, and proposes an access control model SA-TBAC (social attribute and trust based on access control) based on SIoT attributes and trust. By introducing SIoT user trust and dynamic weight function, a more dynamic and flexible trust evaluation mechanism is established, and authorization decision is made according to Bayesian decision theory. Compared with the original model, the dynamic flexibility, security and authorization accuracy of the access control mechanism are enhanced.

3. Model Design

SATBAC model extends the classic attribute-based access control model by incorporating user trust attributes and activity behaviors. Based on this model, it implements a dynamic trust adjustment mechanism and a reliable authorization decision-making method.

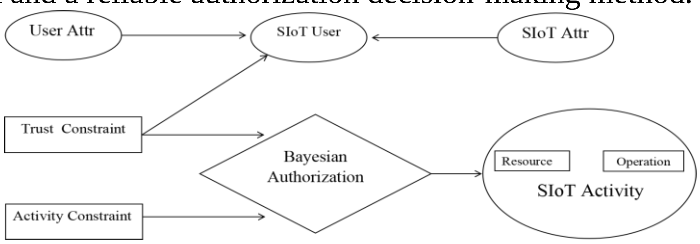

Figure 1: SA-TBAC model.

In SATBAC model, two constraint mechanisms are incorporated: trust constraints and activity constraints. By assessing the trustworthiness of SIoT users, appropriate roles are assigned based on their trust levels, and the specific scenarios in which users perform SIoT activities are considered. This establishes a trust-role-authority mapping relationship, granting users corresponding activity roles and thereby access permissions to execute SIoT activities. The model optimizes the components of trust by aggregating and analyzing intimacy trust, social recommendation trust, and historical interaction trust between nodes from both direct observation and indirect suggestion perspectives, yielding the overall trust level between nodes. Additionally, through dynamic optimization of parameter factors, real-time trust is updated within interaction cycles. A reward and punishment mechanism is introduced to effectively reward friendly nodes and penalize malicious ones during interactions, dynamically adjusting the trust values of SIoT users, ultimately achieving dynamic allocation of access control permissions.

The SA-TBAC model is shown in Figure 1. The model combines the ideas of TBAC model [17] and ABAC model [18], and combines the concept of activity in SIoT, and makes improvements. The parameters in the model are defined below.

Definition 3-1 SIoT Attribute Set SA: Refers to the social relationship attributes between users in the SIoT, which form new types of social relationships based on factors such as location, time, ownership, and inheritance. Specifically, it includes Parent Object Relationship (POR), Co-location Object Relationship (C-LOR), Owner Object Relationship (OOR), Co-time Object Relationship (C-TOR), and Social Object Relationship (SOR).

Definition 3-2 Trust Constraint TC: Calculates the trust level of SIoT users through a trust evaluation model, providing trust values for access authorization Bayesian decision-making. The trust level ranges from [0,1].

Definition 3-3 Activity: An activity refers to the current state of a user, indicating specific operational behaviors that the user is currently performing or will perform, including operations and resources. A user can perform a single activity or multiple activities simultaneously.

Definition 3-4 Activity Constraint AC: Includes type constraints, dependency constraints, and operational constraints. Type constraints refer to the fact that when an SIoT user initiates an access request, it essentially involves executing an SIoT activity, classified by the type of activity to be performed. This paper categorizes SIoT activities into four types: usage, service, control, and decision as shown in Table 1.

Table 1: SIoT Activity Constrait.

Activity level-G	Activity type	Activity privilege
1	usage	read-only
2	service	read and write
3	control	execute
4	decision	grant

In the access control mechanism, authorization is based on constraints and rules. The constraint is mainly to prevent malicious or illegal nodes from dishonest or unauthorized access, which makes the SIoT system suffer losses. The essence of the constraint is to standardize the management of access rights, that is, to implement the optimal decision on the node, to give appropriate permissions, while improving the security of the system, to ensure confidentiality, integrity and availability. Assuming that there is no mutually exclusive relationship between user trust and activity execution in social IoT access interaction, the following two constraints are established: trust-activity constraint and activity-permission constraint.

Trust-Activity Constraint(TAC): TAC is a binary relation defined from the set of trust levels to the set of SIoT activity levels. TAC is established by SIoT users based on their access control requirements for resources or data, adhering to the principle that "high trust corresponds to high-level activities, and low trust corresponds to low-level activities."

Activity-Permission Constraint(APC): APC is a binary relationship defined from the activity level to a set of permissions. As is the trust level of the SIoT user, ps is the level of activity that the SIoT user needs to perform, and it is said that as and ps satisfy APC.APC is determined by SIoT customers or systems based on their own security needs and the sensitivity of various atomic permissions, where in high-sensitivity permissions indicate that the activities performed are of a higher level.

4. Adaptive Access Control Based on the SATBAC Model

4.1. Trust Aggregation of Hybrid SIoT Attributes and User Behaviors

The classical Trust ACM model divides trust into three components: direct trust, indirect trust, and reputation. This paper builds upon that model and tailors it to the specific scenarios of social Internet of Things (SIoT). It identifies the evaluation factors for trust as friendship, interests, and cooperative interactions. By calculating trust, we obtain both direct and indirect trust for SIoT, which are then aggregated to derive the overall SIoT trust.

The interactive trust based on user behavior, together with the SIoT trust, constitutes the user's comprehensive trust. By selecting an appropriate dynamic adjustment function, we can adaptively adjust the proportion of SIoT trust within the comprehensive trust, thereby implementing a dynamically adjustable trust evaluation mechanism. Additionally, a reward and punishment mechanism is introduced to impose strict penalties on malicious interactions while providing moderate rewards for friendly interactions. The trust evaluation for SIoT users is based on trust assessment evidence, which hierarchically describes the composition and sources of trust assessment factors. This is divided into three sources, and described in detail below.

4.1.1. SIoT Trust Level

In current research on SIoT trust, models are generally based on SIoT social relationships to implement effective trust evaluation and aggregation. According to Atzor's definition, SIoT objects can establish various social relationships. This paper conducts a fine-grained classification of SIoT social relationships, utilizing Parent Object Relationship (POR), Owner Object Relationship (OOR), and Co-occurrence Object Relationship (C-LOR) to describe SIoT trust level.

Definition 4-1 Friendship Similarity (FS): This refers to the ratio of the number of mutual friends between users to the total number of friends a user has. A larger ratio indicates a higher degree of friendship.

Definition 4-2 Interest Similarity (IS): This refers to the ratio of the number of shared interests between users in the SIoT to the total number of interests a user has. A larger ratio indicates a higher level of interest similarity.

In the SIoT system, trust evaluation is primarily established through two approaches: direct observation and indirect recommendation. Direct trust is quantified by analyzing the friendship similarity between users, while indirect trust is derived from calculating interest similarity. Specifically, direct trust reflects the trust level based on social relationships between nodes, whereas indirect trust represents the trust established through shared interests. The direct trust value is denoted as STrust, and its computation process can be implemented using the node relationship matrix, as demonstrated in the following formula.

$$\mathrm{S}Trust_{\mathrm{ij}}^{FS}=\frac{|OR_i \cap OR_j|}{|OR_i \cup OR_j|} \tag{1}$$

Indirect recommendations are derived from the social interest sets among nodes. The establishment of social interests typically involves location and inheritance relationships. Consequently, constructing the social interest relationship matrix requires joint computation of the POR and CLOR relationship matrices. The calculation method for SIoT indirect trust is presented below.

$$STrust_{\mathrm{ij}}^{\mathrm{IS}} = \frac{|IS_i \cap IS_j|}{|IS_i \cup IS_j|} \tag{2}$$

Here, IS represents the social interest set of node i, which can be obtained by computing the joint relationship matrix of POR and CLOR.

$$IS_i = POR_i .* CLOR_i \tag{3}$$

Upon completion of the direct and indirect trust computations, an appropriate weighting factor is selected to aggregate these trust values. This paper employs a linear combination approach to calculate the SIoT trust value for users.

$$STrust_{ij}^{S} = \gamma \times STrust_{ij}^{FS} + (1-\gamma) \times STrust_{ij}^{IS} \tag{4}$$

Here, parameter serves as an adjustment factor, whose value is determined by the system's subjective recognition of the intimacy between users and their social interests. When users deem intimacy more trustworthy than interest recommendations, the factor will exceed 0.5.

4.1.2. User Behavior Trustworthiness

In the classic Trust ACM model in [23] and traditional trust evaluation mechanisms, trust establishment in the Social Internet of Things (SIoT) is typically achieved through a single aggregation of direct and indirect trust. In the SATBAC model, the impact of user interaction behavior on comprehensive trust is equally significant. Additionally, based on the principle of minimal disturbance, when user interaction trust reaches a certain number of interactions, initialization of interaction trust is required before the interaction success rate and the number of interactions between nodes reach the threshold. This mechanism aims to prevent interference in the evaluation of interaction trust caused by insufficient interaction counts between nodes. The formula for calculating historical interaction trust between nodes is as follows.

$$STrust_{ij}^{HA} = \begin{cases} 0.5, N \leq t \\ sucess-rate(N-t), N \geq t \end{cases} \tag{5}$$

Here, success-rate(N-t, N) represents the user's interaction success rate from the (N-t)th to the Nth interaction, where N denotes the total number of user interactions.

This paper considers the historical collaboration efficiency between users as an indicator of interaction behavior trust: when the number of interactions falls below a certain threshold, the conditions for cooperation are not met; however, once the number of interactions reaches a certain level, the trust between users is determined by the interaction success rate between nodes.

Trust Reward and Penalty Mechanism: When a trusted node performs friendly or malicious access, its trust value will be dynamically adjusted according to the following function.

$$\delta(N) = \begin{cases} \sigma / 200 * \sin(N * \pi / 200), \mathrm{Re}\, ward \\ \beta / 200 * \cos(N * \pi / 200), Penalty \end{cases} \tag{6}$$

Parameter sigma and beta represent the reward and penalty factors, respectively. Typically, the penalty factor is greater than the reward factor. In practical Social Internet of Things (SIoT) applications, the damage caused by malicious nodes or malicious behavior often results in significant losses to the system.

SIoT environment is inherently open, allowing interactions between users, between users and devices, and between devices themselves. Therefore, conducting effective and objective trust calculations for SIoT nodes and using the resulting trust values as a critical basis for Bayesian-based authorization is essential.

4.1.3. Comprehensive Trust Degree Calculation

This paper addresses the characteristics of SIoT users' interactive behaviors within a cycle, where the weight of behavioral trust in the comprehensive trust degree continuously changes with the increase in interaction frequency. By introducing dynamic parameter adjustments, it achieves dynamic and adaptive evaluation of users' comprehensive trust. Initially, SIoT trust plays a dominant role in access interactions. However, as the number of access interactions increases, the proportion of user behavioral trust in the comprehensive trust gradually rises. Therefore, a functional relationship is established between dynamic parameters and interaction frequency, and the weight-interaction function is introduced as follows.

$$\alpha(N) = 1/\pi * \arctan(5*(T-N)/N) \tag{7}$$

In the calculation of the comprehensive trust degree for SIoT users, the SIoT trust and user behavioral trust are linearly combined, where N represents the number of interactions and T denotes the total number of interactions within the period. The formula for computing the comprehensive trust degree is as follows.

$$STrust(N) = (1-\alpha(N)) * STrust_{ij}^{HA} + \alpha(N) * STrust_{ij}^{S} \tag{8}$$

Here, parameter is the adjustment factor for SIoT trust and behavioral interaction trust, with a value range of [0, 1]. It represents the degree of influence of interaction outcomes on trust composition within the interaction cycle. As the interaction success rate increases, the factor gradually approaches 1.

4.2. Trust-Authorization Constraints

This paper applies Bayesian classification theory to the access authorization process, transforming the problem of trust-based access policy selection into a binary classification problem where trust falls within the authorization policy space. After users obtain corresponding permissions, the accuracy of authorization is analyzed through the Bayesian decision analysis module.

To implement trust-based authorization category decisions for SIoT users using Bayesian decision theory, two fundamental conditions must be met: First, the prior probabilities of user trust levels for different access policy categories must be known, along with the mechanism by which access policy categories influence user trust. Second, the number of policy classification categories must be fixed. Assuming that the trust values between users exceed the system-defined threshold and the trust space of the object is determined, the class-conditional probability density distribution of authorization behaviors falling into the corresponding trust level is known. Under these conditions, the basic requirements of Bayesian decision theory are satisfied. Consequently, the problem of trust-based authorization in SIoT is transformed into the selection of authorization policies based on SIoT user trust levels.

Let the authorization decision set consist of N decision types, with class-conditional probabilities set according to the practical requirements of the SIoT scenario. The system calculates and compares the N posterior probabilities, selecting the decision category corresponding to the maximum probability as the final authorization result.

5. Case Analysis and Experimental Validation

5.1. Case Analysis

Given the limited application of SIoT in actual environments, this study conducts case analysis through simulated real-world scenarios to validate the feasibility and effectiveness of the proposed method in Figure 2. Taking smart healthcare as an example, we designed a comprehensive SIoT activity process that covers three core components: online registration (Register), physical examination and review (Check), and medical diagnosis (Inquiry). This case integrates various SIoT behavioral characteristics, fully demonstrating the practical application value of the proposed method.

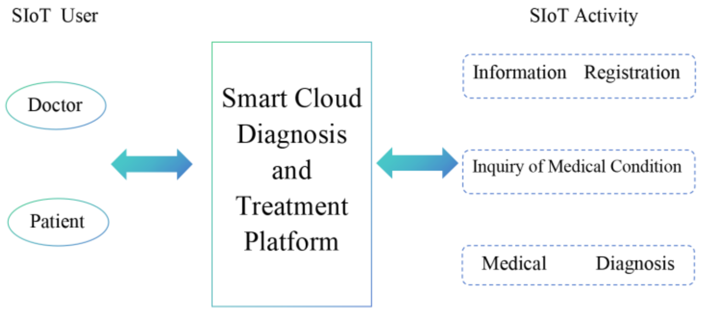

Figure 2: Smart Healthcare Interaction Scenario.

During the cloud-based diagnosis and treatment process, three main types of SIoT activities are conducted between the supervising physician and the patient: Usage Activity (UA), which involves collecting data from the patient's monitoring devices; Control Activity (CA), which adjusts the medical parameters of the patient's devices; and Service Activity (SA), which provides remote medical services. In this context, the physician acts as the interaction subject, while the patient serves as the interaction object. The relationship between the subject and the object is established through three types of social connections: OOR, POR, and CLOR. These relationships are further distinguished by user attributes such as device type, brand, and manufacturer. The devices can collaboratively execute SIoT activities, which are sequentially dependent on one another.

Within a single diagnosis and treatment cycle, multiple interactions are required between the subject and the object, initiated primarily by their respective SIoT devices. The total number of interactions in each cycle is fixed at 200, with the initial interaction requiring the execution of the Register process. In the smart healthcare process, Check (physical examination and review) is the most frequently occurring activity. Once sufficient patient information is obtained, the system initiates the Inquiry (consultation and diagnosis) process, ultimately providing the patient with a diagnosis and treatment outcome. Through this series of processes, both parties complete all the steps within the medical SIoT activity set.

Table 2: Subject SIoT Activity Request Requirements Table.

SIoT Activity	Requested Operation	Activity Type
Register	read upload	SA
Check	read upload download modify	UA SA
Inquiry	read upload download modify delete	CA

In this SIoT scenario, the parameters of SIoT activities, requested operations, and activity types initiated by SIoT users are detailed in Table 2. The SIoT activity types, trust constraints, and activity constraints are outlined in Table 3.

Table 3: Constraint Rules.

TAC	Trust Constraint	Permission Constraint
(1,0)	Not required	read download
(2,0.4)	0.4	read upload download modify
(3,0.8)	0.8	read upload download modify delete

5.2. Experimental Validation

5.2.1. Model safety and interaction success rate

To mitigate the impact of malicious nodes on objects in access control and enhance the accuracy and effectiveness of interactions, this paper implements a trust-based access control model and conducts extensive experiments. The simulation environment is similar to that described in reference [19]. In the Social Internet of Things (SIoT) environment, the initial trust value of access nodes is set to 0.3. The percentages of malicious nodes are varied at 0.1,0.2, 0.3, 0.4, 0.5, 0.6, and 0.7. Each cycle consists of 200 interaction attempts.

Definition 5-1 Interaction Efficiency Rate: This refers to the ratio, within each cycle, of successful interactions—where friendly nodes are granted access and malicious nodes are denied—to the total number of interactions. The interaction efficiency rate is thus defined as the number of effective interactions divided by the total number of interactions.

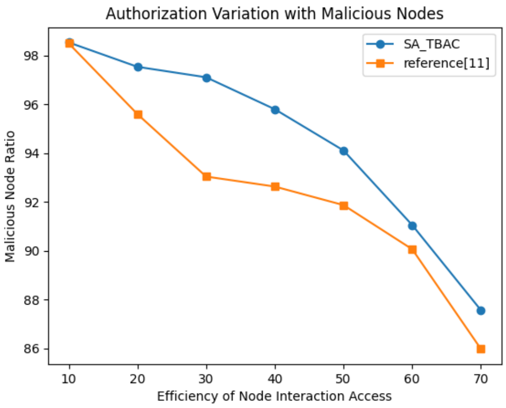

Figure 3: Authorization Changes with Malicious Node Variations.

As shown in Figure 3, this paper compares and analyzes the success rates of interactive authorization between the proposed method and the method in reference [11] as the proportion of malicious nodes varies. From the results, it can be observed that the proposed method maintains a higher interaction success rate across all proportions of malicious nodes. The accuracy and effectiveness of authorization are superior to those of the referenced method.

5.2.2. Fine-Grained Authorization and Dynamic Permission Changes

To verify the fine-grained nature of authorization through experiments, the simulation environment remains the same as before, with an interaction cycle of 200 iterations and a trust evaluation adjustment factor set to be dynamically adjustable. The initial trust level of the subject user is 0.3. In a trustworthy environment, as friendly interactions continue, the user's trust level gradually increases. The object has trust level constraints on SIoT activities. In the initial stage of access, the subject only has the qualification to perform SA. However, as the number of interactions increases and the user's trust level rises, when the trust level reaches 0.4 at N=55, the user gains the qualification to perform UA . When the trust value reaches 0.8 at 130 interactions, the user obtains the permission to perform CA. Based on the sensitivity of permissions, a permission ranking table is derived as follows: read download upload modify delete.

Table 4: Permission Acquisition Results Within Interaction Cycle.

Numbers	Register	Check	Inquiry
[0, 55]	read download	read download	read download
[55, 130]	read download	read download	read download
[130,200]	read download	read upload download	read upload download delete modify

From Table 4, it can be observed that the subject performs the Register activity. Due to the friendly environment, the trust level is 0.3, which meets the trust threshold of UA. Additionally, the expected authorized operations by the object for UA are {read, download}. In this case, the subject can obtain the corresponding permissions, while the upload permission is not granted. The Check activity has a higher trust threshold expectation. When N=55, the trust threshold of 0.4 is achieved. At this point, the subject's requested permissions align with the constraints of the SA activity by the object, and the subject obtains {read, upload, download}. The Inquiry activity involves constraints related to the CA activity, requiring a higher user trust level. When N=110, the expected threshold is reached, and the subject obtains the higher-level delete permission. These examples and the final authorization results, from the perspective of trust-activity-permission, achieve fine-grained authorization based on permission quantity, adhering to the principle of "low-trust users–low-risk activities–low-level-permissions, high-trust users–high-risk tasks–high-level permissions.

Assume that in the TRBAC(Task-Role-Based Access Control) model, before the interaction, the user's trust level has already met the criteria for obtaining the corresponding role, meaning the user has been assigned a role with 4 permissions. In the Register activity, the trust role has already been granted before the interaction, and the permissions remain unchanged throughout the interaction cycle. In contrast, the method proposed in reference [18] dynamically calculates trust values in real-time within a trusted environment, enabling permission granting based on real-time trust values. The approach presented in this paper considers the interaction purpose and the requirements of the object. In the Register activity, a permission count of 2 is sufficient to meet the interaction purpose, adhering to the principle of least privilege. Similarly, in the Check and Inquiry activities, while implementing dynamic authorization based on real-time trust values, the method also achieves fine-grained permission granting based on the interaction purpose, with the permission count varying within the interaction cycle.

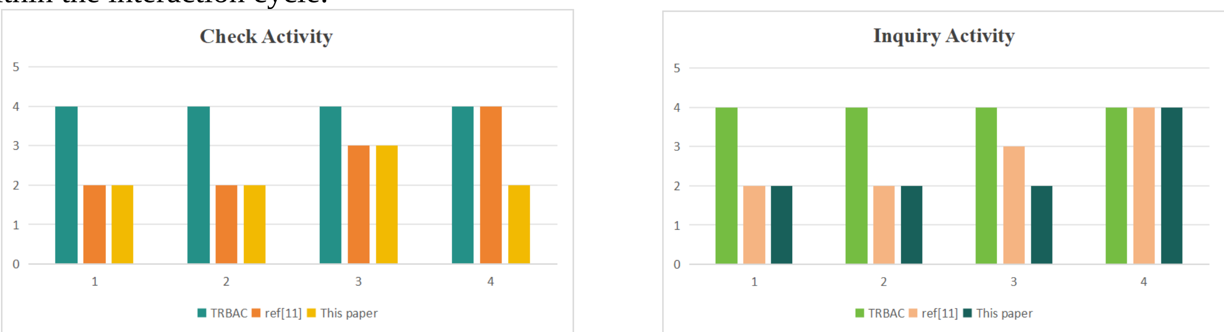

Figure 4: Smart Healthcare Interaction Scenario.

As shown in Figure 4, the number of access permissions changes during different phases of the interaction cycle. In the TRBAC model, based on the pre-established trust-role-permission relationship, users are granted permanent permissions, and the number of permissions remains constant across all interaction phases. Zhao et al. [11] establishes a direct mapping between trust and permissions, enabling flexible fine-grained authorization. In this method, as trust values increase over different interaction cycles, higher-trust nodes are gradually granted more permissions. Building on the strengths of these two models, the method proposed in this paper further incorporates the access requirements of different interaction phases, implementing more dynamic and fine-grained permission granting based on the interaction purpose.

Table 5: Comprehensive Trust Evaluation Evidence for SIoT Users.

Models	Decision Method	Dynamic Adjustment	Trust Composition	Decision Accuracy	Dynamic Self-Adaptation
Zhao et al. [11]	Role	None	None	High	None
Zhang et al.[14]	Game Theory	None	None	Relatively High	High
Pan et al. [21]	Attribute	Yes	User Trust	High	Relatively Low
Zhang et al.[24]	Game Theory	Yes	User Trust	General	Relatively Low
This paper	Bayesian Decision	Yes	SIoT Trust and User Trust	High	Relatively High

A comparison between the proposed method and the aforementioned related works is conducted in terms of decision-making approach, dynamic trust adjustment, trust composition, authorization accuracy, and dynamic adaptability. The comparison results are summarized in Table 5.

6. Conclusion

To address security concerns in the SIoT environment and enhance effective interactions among legitimate nodes, this study proposes a dynamic access control authorization mechanism based on SIoT trust. Unlike traditional access control models that rely on fixed weight factors for dynamic evaluation, this mechanism introduces dynamic weight factors to refine the trust assessment process. Additionally, it establishes a robust constraint and decision-making framework to improve the access authorization system. Post-authorization, the mechanism implements fine-grained control by verifying interaction purposes against expected trust levels. Experimental results demonstrate that the proposed model effectively integrates trust evaluation with decision authorization, significantly improves the detection rate of malicious nodes, and enables appropriate fine-grained authorization for various interaction types.

Acknowledgements

This study was supported by the Xinjiang College of Science and Technology Natural Science Foundation under grant No.2024-KYPT3.

References

[1] Atzori L., Iera A., Morabito G. (2011). SIoT: Giving a social structure to the internet of things. IEEE Communications Letters, 15(11),1193-1195.

[2] Mi B., Liang X., Zhang S. (2018). A Review of Research on Social Internet of Things. Chinese Journal of Computers,41(07,1448-1475.

[3] Kamilaris A., Pitsillides A. (2010). Social networking of the smart home[C]// IEEE International Symposium on Personal Indoor and Mobile Radio Communications. IEEE.

[4] Kang D., Choi J., Jung J. (2016). SDIF : Social device interaction framework for encounter and play in smart home service. IEEE Transactions on Consumer Electronics, 62(1), 85-93.

[5] Diazsanchez D., Marin A., Almenarez F. (2010). Social applications in the home network. IEEE Transactions on Consumer Electronics, 56(1), 220-225.

[6] Atzori L., Iera A., Morabito G. (2012). The social internet of things (SIoT) - when social networks meet the internet of things: concept, architecture and network characterization. Computer networks, (16),56.
[7] Shaji S., Ramesh M., Menon V. (2016). Real-Time processing and analysis for activity classification to enhance wearable wireless ECG. Springer India.
[8] Gupta M., Sandhu R. (2021). Towards activity-centric access control for smart collaborative ecosystems [C] // Proceedings of the 26th ACM Symposium on Access Control Models and Technologies. 155-164.
[9] Alam K., Saini M., Saddik A. (2015). Toward social internet of vehicles: concept, architecture, and applications. IEEE Access, 3,343-357.
[10] Floris A., Nitti M., Girau R., et al. (2014). On adding the social dimension to the internet of vehicles: Friendship and middleware[C]// IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), IEEE.
[11] Zhao B., He J. (2015). A Risk-Minimization Authorization Mapping Method Based on Bayesian Decision Theory. Chinese Journal of Communications, 36(S1), 157-161.
[12] Wu J., Dong M., Ota K. (2014). A fine-grained cross-domain access control mechanism for social internet of things[C] 2014 IEEE 11th Intl Conf on Ubiquitous Intelligence and Computing and 2014 IEEE 11th Intl Conf on Autonomic and Trusted Computing and 2014 IEEE 14th Intl Conf on Scalable Computing and Communications and Its Associated Workshops. IEEE, 666-671.
[13] Chang G., Liu Y., Ye Q. (2017). An attribute-based fine-grained access control scheme in vehicular ad-hoc networks. Wireless Communications, Networking and Applications.
[14] Zhang H., Ma P., Liu B. (2021). Adaptive fine-grained access control method in social internet of things. International Journal of Network Security, 23(1), 42-48.
[15] Deng S., Yuan L., Sun L. (2022). Research on IoT Access Control Model Based on Trust Degree. Computer Engineering and Design, 43(11), 3030-3036
[16] Qiao Y., Xu D., Dai G. (2000). A New Model of Role-Based Access Control (RBAC) and Its Implementation Mechanism. Journal of Computer Research and Development, (01), 37-44.
[17] Liu W., Duan H., Zhang H., Ren P., Wu J. (2011). TRBAC: A Trust-Based Access Control Model. Chinese Journal of Computer Research and Development, 48(08), 1414-1420.
[18] Li X., Feng D., Chen C., Fang Z. (2008). Attribute-Based Access Control Model. Chinese Journal on Communications, (04), 90-98.
[19] Li Y., Guo H., Peng W., Song C. (2016). Synthesis of Access Control Policies Based on Trust Degree Attributes. Chinese Application Research of Computers,33(07), 2175-2180.
[20] Gong A., Liu H. (2015). P2P Access Control Model Based on Trust Fuzzy Evaluation. Chinese Computer Engineering, 41(03), 125-129.
[21] Pan R., Wang G., Huang H. (2021). Attribute-Based Access Control with Dynamic User Trust Degree in Cloud Computing. Computer Science, 48(05), 313-319.
[22] Zhang Y., Tian L., Wu Z., Wu W. (2021). A Game Mechanism for Trust-Oriented Dynamic Access Control in Cloud Services. Mini-Micro Systems, 42(08), 1774-1779.
[23] Subramanian A., K. S. (2016). CTRAC: A combined trust and recommendation based access control approach for cloud computing. Asian Journal of Research in Social Sciences and Humanities, 6(6).
[24] Oliveira G., Souza B., Nogueira M., Santos A. (2021). An access control for IoT based on network community perception and social trust against sybil attacks. International Journal of Network Management, 32(1).