Adaptive Fine-grained Access Control Method in Social Internet of Things

Hongbin Zhang[1,2], Pengcheng Ma[1], and Bin Liu[3,4]
(Corresponding author: Hongbin Zhang)

School of Information Science and Engineering, Hebei University of Science and Technology[1]
Shijiazhuang, P. R. China
Hebei Key Laboratory of Network and Information Security Hebei Normal[2]
School of Economics and Management, Hebei University of Science[3]
Technology Research Center of Big Data and Social Computing, Hebei University of Science[4]
(Email: hbzhang@live.com)

(Received June 27, 2019; Revised and Accepted Dec. 12, 2019; First Online Feb. 1, 2020)

Abstract

Social Internet of Things (SloT), as a new carrier of integration of social and Internet of Things, applies the research results of social networks from different aspects of the Internet of Things. Different types of connected intelligent objects interact socially, compared with random data access between them, access control technology is more stringent. This paper integrates social attributes into attribute-based access control of Internet of Things, initializes relational attribute tags, and labels social interest attributes for different objects, then quantifies tag similarity and implements initial access control authorization, integrates social attributes into game theory to dynamically adjust access control policies, so the adaptive fine-grained division of access control under the Social Internet of Things is effectively realized. The experimental results show that our method can not only effectively carry out initial authorization according to tag similarity, but also further adaptively adjust the permission policy according to social attributes, and further meet the fine-grained partition requirements of access control, which is ensure the effective implementation of access control under the Social Internet of things.

Keywords: Access control; Dynamic adaptation; Game theory; Social Attributes; Social Internet of Things

1 Introduction

Internet of things is regarded as an important opportunity for development and change in the field of information. The European Commission believes that the development and application of Internet of things will bring great contribution to solving modern social problems in the next 5-15 years. It is estimated that by 2020, there will be 25 billion various things (devices, sensors, software or databases) that can connect to the Internet wirelessly. [1]. Gartners predicts that the number of connected things will be generated by consumer applications, and most of the revenue will be contributed by enterprises. This sudden development will support the Internet of things as the economic effect of consumers, and enterprises will find new ways to use this technology. According to Manyika, by 2025, the use of the Internet of things can create 4-11 trillion economic value, which is equivalent to 11% of the world economy [9].

Social media is an Internet-based technology for sharing ideas, activities and professional interests. The development of the Internet of Things is changing the way social media is used. The daily connection between people, objects and data creates an intelligent network, which adds value to the people involved [12]. The Social Internet of Things adds attributes of social networks to the Internet of Things, analogous to human social networks to define the social relationships between objects in the Internet of Things. The model of social Internet of things is designed, the structure of social network based on objects of the Internet of things is analyzed, so that the model of human social network can be extended to a variety of fields based on things-things ,things-people, people-things and people-people [8].

Heterogeneous devices and information exchange are ubiquitous in the social Internet of things, which requires more effective access control measures for services. Traditional access control based on Internet of Things mostly choose to build trust model and risk model [5]. We propose an access control model in the social Internet of Things, which integrates social attributes into the attribute-based access control model in the Internet of Things. The game theory is used to integrate social attributes to achieve dynamic fine-grained rights partitioning in SloT environment.

The rest of this paper is organized as follows. In Sec-

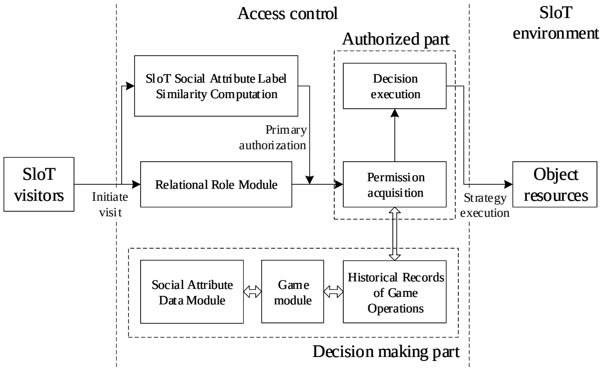

Figure 1: Access control model based on game theory

tion 2, we present the related work. Section 3 gives the preliminaries of this paper. Section 4 describes the access control model and the game process in detail. The 5th section carries on the experiment simulation and the verification as well as the method contrast. We conclude the whole paper in Section 6.

2 Related Work

Social Internet of things as a new integration carrier of social network and Internet of things, through the traditional structure of the Internet of things to add social attributes to achieve the effective operation of social Internet of things scenarios, this paper studies the idea to explore the deeper structure characteristics of the Internet of things and social network attributes based on the integration of access control methods under the current social Internet of things. Through the research of the security problem of the combination of the two, it lays a solid foundation for the research of adaptive fine-grained access control under the social Internet of things.

Social Internet of Things integrates the concepts of the Internet of Things and social networks to integrate social attributes into the huge Internet of Things terminal nodes. Akash Sinha et al proposed a framework of social Internet of Things to support the interaction between devices with different functions and heterogeneous platforms by developing applications that provide effective services for the Internet of Things by utilizing users'social behavior, which can reasonably interact with the social behavior of the Internet of Things. Literature [14]. Literature [15] through the construction of online trust model, classifies the roles of users in social networks and provides threshold trust score, which will be further applied to role allocation. Literature [2] proposes a risk-based access control model for Internet of Things (IOT) technology, which considers real-time data requests of devices in the Internet of Things and gives dynamic feedback. User context, resource sensitivity, action severity and risk history are used as input of the security risk estimation algorithm. By confirming the security risk of the request, a reasonable data basis is proposed for policy formulation. No matter the trust model or the risk model, although there are no research examples of the fusio n attributes in specific scenarios, they have rich research basis in satisfying the social network and the Internet of things scenarios, which provides ideas for the fine-grained access control division under the social Internet of things.

According to the behavior analysis of entities in reference [13] access control can be regarded as a game between requester and visitor, and a dynamic game access control model based on trust is proposed. In this paper, the access of nodes is clearly divided into two types: goodwill and malice, which obviously lacks in the fine-grained access control division work, and the article model is not in the actual access control situation, and there is no clear introduction to the implementation of the model. The trust value of nodes is evaluated according to shared contribution, shared cost and organizational contribution.The Access Control Middleware mentioned in document. The Access Control Middleware mentioned in document [4] not only considers the subject behavior and trust value, but also describes in detail the dynamic adaptation process of an access control policy based on risk value, policy and rule set. Literature [11] proposes a dynamic and fully distributed access control policy in the framework of the Internet of Things. Block chains satisfy the distributed concept of the Internet of Things, which strengthen the construction of dynamic adaptive learning model in line with the environment of the Internet of Things. However, the paper does not quantify the specific implementation of access control strategy, only proposes a conceptual framework model for follow-up. However, the dynamic and effective solution of access control under the blockchain is still of great significance to solve the problem of traditional Internet of things distributed scenarios. research.

3 Preliminaries

As a new social carrier, Social Internet of Things integrates social network concepts into Internet of Things (IoT) solutions to enhance the ability of Internet of Things network services in an objective and effective way. The effective operation of SIoT poses new challenges to the implementation of access control. We propose an access control model based on repeated game in the social Internet of things. The specific block diagram is as Figure 1.

SloT access is directly authorized if it meets the "Special relationship" in the relational role attributes. If it is not, the primary matching authorization is performed according to the SloT social attribute tag similarity. When the visitor initiates the SloT social behavior and triggers the two-party game, the two parties perform multiple repeated games.Each game record is counted into the game operation history record, and the mixed strategy Nash equilibrium calculation is performed according to the game operation history record.

3.1 Relational Attribute Label

Firstly, we divide the access control of nodes according to the similarity of labels, and then adjust the access control adaptively by using game theory according to social attributes. Based on the model. The tag similarity algorithm gives the preliminary division basis of access control.

Definition 1. *User tags are extracted from SloT's social attribute resources, the user tag behavior is represented by a set of triples, where the Ra-data record (v, c, l) indicates that the user (node) v labels the category c with the content l.*

v is the node Id, which is the account identifier of the SloT, and is used to distinguish different accounts

$$v = \{v_1; v_2; \cdots, v_i\},$$

indicating different Id;

c is the node label category, including relationships, roles, interests and other categories; l is the content of the label;

Rr-attribute (Relational role attributes), preliminary role validation and SloT node validity are carried out, which are satisfy the numerical Boolean structure.

The set of degree nodes connected by SloT node v.

$$\mathrm{f}\left(V_{i,}\right) = \left\{V_{ik,}\right\}, \quad \mathrm{k} = 1, 2, \ldots, \mathrm{n}.$$

By independently calibrating the relationship attributes between the nodes, we can get their relationship role attributes eigenvalues:

$$\mathrm{B_i}\left(\mathrm{v_i}\right)\left\{\begin{array}{ll} 1, \text{Coincidence characteristics} \\ 0, \qquad \text{otherwise} \end{array}\right., i = 1, \ldots, n.$$

I is the number of nodes with different relational attributes extracted, For example, $B1$ $(v1)$ is the relationship label information between a subject and an object. If marked as "intimate relationship", you can directly enjoy the highest privileges, but if the account is identified as "bad friends", you can directly exclude it.

3.2 Interest Attribute Label

Din-attribute: SloT node has n dynamic interest labels to define the personalized interest identification of the node for subsequent node interest similarity calculation.

In the SloT environment, facing the access requests of many nodes, the object calculates the initial authorization according to the matching similarity of the labels that the nodes have. In the process of social behavior of SloT, the nodes gradually form their own interest labels. For the account with unexpected loss of interest label attributes, we can generate the personalized interest topic labels of nodes through our improved label propagation algorithm (LPA) [6]. The specific algorithm implementation process is as follows:

Input: Adjacency Matrix of Undirected Unweighted Graph Adjacentmatrix, node number VerticeNum.

Output: Classified array for storing node labels Community.

Step 1: Save all neighbors of the i node into the neighbor array.

Step 2: When the classification criteria are not met or the iteration threshold is not exceeded, the number of tags in the neighborhood of the node is counted.

Step 3: If there is only one tag with the most number, assign the value directly; If there are multiple tags with the same number, select one at random.

Step 4: Determine whether the node label exceeds the iteration threshold, and re-enter if it does not Adjacent matrix, Until you find a community that meets the requirements community.

The object authorizes the nodes according to the Boolean value of the relationship role attribute, and then uses the similarity of interest tags as the authorization basis of other nodes, The similarity of subject and object tags still plays a dynamic role in the ubsequent access control process. The specific calculation process of label similarity is as follows:

Definition 2.

$$\begin{aligned} v_1 &= \left\{l_{i1}, l_{i2}, l_{i3}, \cdots l_{(ik)}\right\} \\ v_2 &= \left\{l_{j1}, l_{i2}, l_{j3}, \ldots l_{(jk)}\right\} \end{aligned}$$

The number of labels $m < k < n$, m and n are both single values. If the value of k is too large, the interest labels of the account nodes may be too broad to be correctly classified into valid permission levels. If the value of k is too small, the fewer the labels, the larger the similarity value is or even close to 1. And we have to further define the weights for the k labels of node v.

Table 1: Account private label corresponding number and its value corresponding table

Label serial number	Value
1	k_v
2	k_{v+1}
...	...
k-1	k_2
k	k_1

List the label vectors with the value, and then calculate the similarity between the two according to the similarity formula. The similarity formula is as following Label similarity:

$$\cos\theta = \frac{v_1 \cdot v_2}{\|v_1\| \, \|v_2\|}$$

4 Game-based Adaptive Access Control Model

In the SloT environment, besides the adaptability of label similarity, the interviewee hope to gain effective interaction from the visitors through reasonable SloT authorization, while the visitors need to pay a certain amount of SloT behavior to gain reasonable authorization from the respondents. Through effective game theory interaction, the two sides can obtain more practical value in accordance with the SloT environment to adapt to dynamic and complex SloT environment. We use the repeated game model to describe the behavior of both the subject and the object (in the game process, in order to show the game relationship between the subject and the object, we call the subject as the visitor and the object as the interviewee). The specific process of the game is as follow:

v: Indicates the player who participates in the game, and only two-party games are considered in our model, that is, the visitor and the interviewee are expressed as $v = \{v_a, v_b\}$.

u: Indicates the profit of both sides of the game, $u = \{u_a, u_b\}$.

In the course of both games, each party will seek to maximize their own interests.

$\beta(\gamma)$: discount factor: $\beta(\gamma) \in [0, 1]$ is the discount factor to control the rate of change of income with time. Which can also be understood as the patience level of the person in the game. In this paper, we take $\beta = \gamma = 1$, $\beta(\gamma)$ represent the discount factor of the visitor and the interviewee respectively.

s: The policy adopted by both sides of the game, that is, the SloT behavior. The visitor needs to pay more and more effective SloT social behavior to obtain higher SloT access rights, while the interviewee needs reasonable authorization, the two parties denoted as $\{s_a, s_b\}$.

The s expenditure (and is also the income of the interviewee) can be divided into n kinds of behaviors

So a total of $s_a == 2^n$ kinds of collection behaviors.

We stipulate that visitors must initiate SloT behavior to trigger the game, that is, the visitor initiates $2^n - 1$ sets containing SloT behaviors.

The interviewee has corresponding $s_b = 2^n - 1$ permission policy selection.

The interviewee expenditure (and is also the income of the visitor).

When the visitor adopts the $2^n - 1$ level SloT behavior, the interviewee gives the permission $2^n - 1$ level to perform repeated games.

When the t-th game is played, the visitors income (the interviewee's expenditure) is as follows

$$U_a = U_a + \beta U_a + \beta^2 U_a + \ldots + \beta^{t-1} U_a = \Sigma_t \beta^{t-1} U_a = t^* U_a$$

T is number of times. When the t-th game is played, the income of the interviewee (the visitors' expenditure) is as

$$U_b = U_b + \gamma U_b + \gamma^2 U_b + \ldots + \gamma^{t-1} U_b = \sum_t \gamma^{t-1} U_b = t^* U_b$$

T is number of times. All of the t repeated games, the final payment matrix can be obtained.

$$\begin{bmatrix} (1,1) & \ldots & (1,n) \\ \vdots & \ddots & \vdots \\ (n,1) & \ldots & (n,n) \end{bmatrix}$$

Through the payment matrix, we can find that visitors have $2^n - 1$ level of SloT behavior, the interviewee has $2^n - 1$ kinds of permission policies, and the interviewee can use game theory to find out The accessibility level of the visitor's best authority is to select the appropriate Nash Equilibrium [10] for authorization according to the game theory.

The above Nash Equilibrium only applies to the specific non-randomness action plan of each player in the pure strategy form, while the mixed strategy Nash Equilibrium shows that the player can randomly select a pure strategy from the pure strategy set according to a certain probability as the actual action. Further elaboration of hybrid Nash equilibrium makes the access control system more effective in adapting to complex and changeable SloT environment.

The probability of a visitor's action in the face of a resource is expressed as a vector form of

$$\text{p} = \{p_1, p_2, \ldots, (1 - p_i)\}$$

The probability of authorization requirement of the interviewee in the face of the visitor is expressed in the vector form of

$$q = \{q_1, q_2, \ldots, (1 - q_i)\}$$

Table 2: Similarity matching value and initial permission level table

Serial number	interviewee	Visitor	Similarity Matching Value	Initial permissions
1	2A50	On3k	0.3337789963679875	2
2	bRlo	r0aw	0.4351501871273176	3
3	5osV	T0jx	0.10745062398909976	1
4	CRqw	eS2B	0.74527581901392475	4
5	z2wn	N4Gk	0.9611650085651615	5

Visitors' expectations are represented by the hierarchical value $c = \{c_1, c_2, \ldots, c_i\}$ of each level of the diagonal matrix.

The expected value of the interviewee is expressed in the diagonal value $\mathrm{d} = \{\mathrm{d}_1, \mathrm{d}_2, \ldots, \mathrm{d}_\mathrm{i}\}$ of each level of the matrix.

Visitors' expected payment is

$$EU_a = c_1 * p_1 + c_1 * p_2 + \ldots + c_i * (1 - p_{i-1}) .$$

Interviewee's expected payment is

$$EU_b = \mathrm{d}_1 * q_1 + \mathrm{d}_2 * q_2 + \ldots + \mathrm{d}_\mathrm{i} * (1 - q_{i-1}) .$$

In game theory, there are only two players, the visitor and the interviewee, but each player has a variety of strategic options, so we can calculate the expected payment of each person's mixed strategy Nash equilibrium in the face of complex situations, in order to adapt to the more dynamic and changeable SloT environment.

5 Experimental Simulation And Verification

We assume that there are 100 Id sources, each node has its own content tags of $l = 6$ from social attributes, and that there are $n = 4$ kinds SloT behaviors for visitors, then there are a total of $s = 4^2 - 1$ policy choices for the Interviewee. Our content tags based on social attributes originate from a social networking site in China. The weights of six tags are calculated according to the current ranking of the calorific value of the tag in the overall website. Our experiment sets that the weights of each Id tag are ranked according to its calorific value on the website.

Normalization method can well normalize all Id label weight values, reduce the influence of large eigenvalues on the difference between vectors, and eliminate the imbalance caused by the difference between attributes. In the calculation of node label weight, the raw data is linearly transformed using the standardization method of dispersion:

$$x' = \frac{(x - \min)}{\max - \min}$$

In order to reflect individual differences, we randomly selected 30 Id from 100 Id sources as visitors'Ids, matched the remaining 99 Ids with label similarity, and randomly selected 5 groups as our experimental objects, giving the result as Table 2.

From Table 2, we can see that our adaptive model initially authorizes visitors according to their interest tags, allowing them to read part of the interviewee's resources. Through the study of literature [3, 7], we can know that the social behavior of online visitors meets a certain degree of Gauss distribution, so we analyze the online social behavior of some users of a domestic website, and randomly select some users and related data as the behavior basis of our method.

$$\mu = \frac{X}{N}$$

$$\sigma = \sqrt{\frac{\Sigma(X - \mu)^2}{N}}$$

σ is the standard deviation, X is the variable, μ is the total mean, and N is the total number of cases.

We take the two groups of 1-3 groups as examples. The visitor's access behavior satisfies the Gaussian distribution, but in the early stage of the experiment, we must manually remove some nodes with larger differences, corresponding to the right oblique upper triangle the lower left triangle of the payment matrix. We consider that the difference $\geqslant 5$ in the two-dimensional array is the point of great difference, which can be removed manually. Three groups of visitors were randomly selected from a certain platform to verify our experiment on the premise that their online social behavior meets the following requirements.

The 15*15 payment mmatrix of game parties based on our experimental simulation, we can easily find that the diagonal line of the matrix belongs to the ultimate ideal state of our game. Since we initially excluded the difference $\geqslant 5$ in the expected payment two-dimensional array, we left a total of 9 diagonal data in the order of 1-9 from bottom to top, then the final expectation such as the distribution in the table, that is, the visitors matched the income permissions corresponding to their own efforts, so our method was verified, and the model can adapt dynamically according to the behavior subject and object to form an effective adaptive adjustment and fine-grained access control division

$$\begin{bmatrix} (1,1) & \ldots & (1,15) \\ \vdots & \ddots & \vdots \\ (15,1) & \cdots & (15,15) \end{bmatrix}$$

Table 3: Similarity matching value and initial permission level table

Number of visits Visitor situation	5	10	15	20	30	40
μ=4.1, δ=2.43	5.1085	4.7077	5.5986	5.6388	5.7460	5.7470
μ=7.32, δ=3.62	4.2548	5.9819	5.0096	6.0772	6.8670	6.7359
μ=2.18, δ=2.76	6.8614	6.1879	4.6837	5.2983	5.7629	5.8656

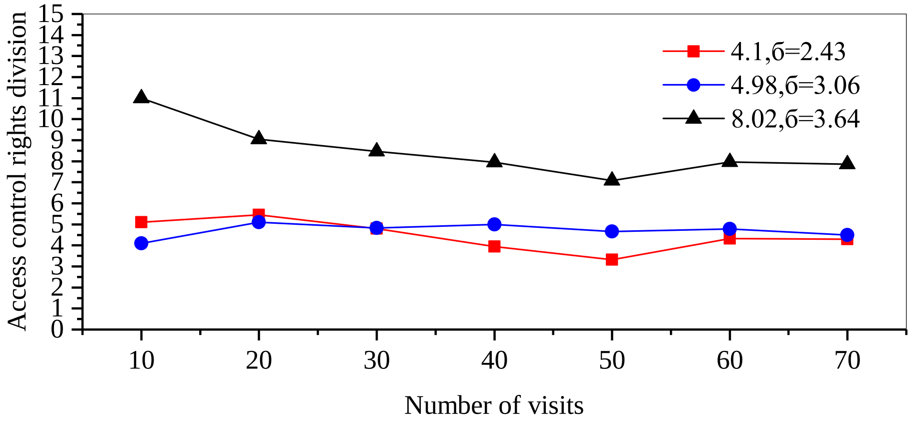

Figure 2: Access control adaptive state diagram

In our experiment, we initially authorized visitors based on tag similarity, but at the same time, similarity tags still play an important role in subsequent visitors. The third is the adaptive adjustment process of the experimental group as shown in the figure.

According to Figures 2, we can see that the experimental group starts with the initial permissions, which are granted according to the label similarity of the nodes. With the social behavior of the visitors, the double access control game is triggered. Combined with the social behavior of the visitors conforming to the Gauss distribution, the authorization strategy of the visitors gradually stabilizes, and the access control model passes through both sides. The multiple game gradually adapts to the strategies of both parties, and forms the reference basis for the access control behavior of both the subject and the object.It can be further seen from Figure 2 that at the beginning of accessing resources, the three groups of visitors have respectively obtained levels 1-3 preliminary access rights according to their own tag similarity. With the implementation of the adaptive model, they have achieved levels 1-5, levels 2-5, levels 3-7 adaptive comparison display.

6 Conclusions And Future Work

Referring to the traditional attribute-based access control model in the Internet of Things, this paper effectively integrates the social attributes of nodes and constructs a reasonable access control strategy by using game theory, which effectively guarantees the dynamic fine-grained adjustment of access control schemes in the Internet of Things. Experiments show that the model can not only preliminarily authorize based on label similarity, but also dynamically adjust access control strategies according to social attributes, which achieve fine-grained partitioning of policies. In the next step, we introduce the topic of how to dynamically and adaptively adjust social attribute tags into our access control framework. which will provide an effective theoretical and experimental basis for further implementation of access control in the social Internet of things.

Acknowledgements

This research was supported by the National Natural Science Foundation of China (61672206,61572170), Hebei Province Science and Technology Support Program (17210104D), Hebei Province Innovation Capacity Improvement Program Soft Science Research and Science Popularization Project (17K50702D), College Science and Technology Research Project of Heibei Province (ZD2015099).

References

[1] Z. Andrea, B. Nicola, C. Angelo, V. Lorenzo, and Z. Michele, "Internet of things for smart cities," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 22–32, 2014.

[2] H. F. Atlam, A. Alenezi, R. K. Hussein, and G. B. Wills, "Validation of an adaptive risk-based access control model for the internet of things," in *International Journal of Computer Network and Information Security*, vol. 1, pp. 26–35, 2018.

[3] X. Dong, H. Sandra, and C. Ming, "Opinion behavior analysis in social networks under the influence of coopetitive media," vol. PP, no. 99, pp. 1–1, 2019.

[4] O. Hamdi, A. N. Ben, and S. L. Ben, "Towards a self-adaptive access control middleware for the internet of things," in *International Conference on Information Networking*, 2018. DOI: 10.1109/ICOIN.2018.8343178.

[5] B. Lee, R. Vanickis, F. Rogelio, and P. Jacob, "Situational awareness based risk-adaptable access control in enterprise networks," in *The 2nd International Conference on Internet of Things, Big Data and Security (IoTBDS'17)*, pp. 400–405, 2017.

[6] W. Li, H. Ce, M. Wang, and X. Chen, "Stepping community detection algorithm based on label propagation and similarity," *Physica A Statistical Mechanics and Its Applications*, vol. 472, pp. 145–155, 2017.

[7] Q. Liu, Q. Liu, L. Yang, and G. Wang, "A multi-granularity collective behavior analysis approach for online social networks," *Granular Computing*, vol. 3, no. 4, pp. 333–343, 2018.

[8] A. Luigi, C. Davide, and I. Antonio, "Smart things in the social loop: Paradigms, technologies, and potentials," *Ad Hoc Networks*, vol. 18, no. 7, pp. 121–132, 2014.

[9] J. Manyika, M. Chui, P. Bisson, J. Woetzel, R. Dobbs, J. Bughin, and D. Aharon, *Unlocking the Potential of the Internet of Things*, 2015. (https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world)

[10] J. F. Nash, "Equilibrium points in n-person games," *Proceedings of the National Academy of Sciences of the United States of America*, vol. 36, no. 1, pp. 48–49, 1950.

[11] A. Outchakoucht, H. Es-Samaali, and J. Philippe, "Dynamic access control policy based on blockchain and machine learning for the internet of things," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 7, pp. 417–424, 2017.

[12] A. Sabri, "A proposed social web of things business framework," in *International Conference on Engineering and Technology (ICET'17)*, pp. 1–5, 2017.

[13] M. Shunan, "Dynamic game access control based on trust," in *IEEE Trustcom/BigDataSE/ISPA*, 2015. DOI: 10.1109/Trustcom.2015.532.

[14] A. Sinha and P. Kumar, "A novel framework for social internet of things," *Indian Journal of Science and Technology*, vol. 9, no. 36, 2016.

[15] T. Vedashree and N. M. Parikshit, "Trust-based access control in multi-role environment of online social networks," *Wireless Personal Communications*, no. 1, pp. 1–9, 2018.

Biography

Hongbin Zhang is an Associate Professor of the School of Information Science and Engineering at the HEBUST, he received his BS degree from the Department of Automation at HEBUST in 1998, his MEng and PhD degrees from the School of Computer Science and Technology at the Xidian University in 2005 and 2009, respectively. His current research interests include security and management of network, insider threat analysis, etc

Pengcheng Ma is a graduate student of Hebei University of Science and Technology, majoring in Internet of Things security and management during his postgraduate period, and has published two papers in related fields.

Yan Zhang 23 years old, an undergraduate from Shenyang Normal University, major in information security management. In the four years of college, after completing her studies, she enjoys reading the book related to this major. Under the guidance of the teacher, she has published two articles in EI journals.23 years old, an undergraduate from Shenyang Normal University, major in information security management. In the four years of college, after completing her studies, she enjoys reading the book related to this major. Under the guidance of the teacher, she has published two articles in EI journals.