LETTER

Privacy-Preserving Model of IoT Based Trust Evaluation

Zhenguo CHEN[†a)], ***Member and*** **Liqin TIAN**[††b)], ***Nonmember***

SUMMARY With the popularization of Internet of things (IoT), the interaction between human and IoT has become a daily life. In this interaction, the objects of IoT usually require access to personal data, which are often sensitive. We propose a lightweight privacy-preserving model based on the trust evaluation that it can effectively protect privacy based on simple threshold detection. The key issue we address in this work is how to construct trust model so that non trusted objects were prevented from accessing private data. This work can be considered as a lightweight approach to access control for privacy-preservation. The main algorithm in the proposed model is a kind of dynamic self-adjusting trust evaluation mechanism that uses a combination of interaction information occurs between the human and the Internet of things, between the human and the human. According to the given threshold, the trust model can determine the data level of object access in the IoT. We have implemented a prototype of the proposed scheme, thereby demonstrating the feasibility of the proposed scheme on resource-constrained devices.

key words: *privacy-preserving, Internet of things, trust evaluation, data security*

1. Introduction

The development of the Internet of things (IoT) has greatly influenced the production and daily lives of human. In recent years, the research and application of the IoT have gained wide attention. The field and scope of interaction between human and IoT has become increasingly widespread. The nodes of IoT are everywhere, and that is to say the human's privacy data is extremely easy to get. So the challenge which must be overcome before widespread deployment of IoT that relies on objects of IoT is trusted [1], [2].

The motivation in this work is based on the interaction that the trust value of object can be provisioned based on the process of interaction. For example, consider the case of an unknown object that it wants get private data from a person if the trust value of object has crossed specific thresholds. In fact, any form of application scenarios that involve anomaly access can be supported by such a framework.

Privacy-Preserving model consists of three components: trust evaluation module, privacy classification module and access control module. The cautious control strategy is adopted. The unknown object is considered to be not trusted. In the model, three thresholds are set. Each threshold corresponds to a data privacy level. According to the trust value and the threshold value, we can control the data of the object access.

Our proposal has the following advantages. First, the realization is simple, easy to deploy in resource constrained device. Second, trust value is dynamic and can cope with the changing environment.

Our privacy-preserving design can be considered as a simple form of access control. The basis of control depends on the degree of trust between the interacting objects. The computation and storage of trust value are all located on the intelligent devices which are carried by human. Object of IoT is only involved in the calculation of direct interaction trust. Therefore, the reliability of the trust value is guaranteed.

Privacy-preserving is not a new issue. Privacy-preserving methods have been extensively used in data publishing, data mining, location-based services, data aggregation, and other areas. In the process of popularization of Internet of things technology, the problem of privacy protection has encountered a lot of new situations and challenges. In recent years, many scholars began to study it to solve the privacy issues, and have achieved some results [3]–[7].

All the above privacy-related works, whether related to IoT or not, do not take into account the role of interaction behavior and human initiative in privacy protection. Of course, there are some consideration to the participants of the initiative, and put forward some protection scheme.

2. Privacy-Preserving Model

2.1 Design of Trust Evaluation Module

Trust evaluation module is composed of three parts, which are direct interactive trust, friend recommendation trust and historical trust.

Trust evaluation is the basis of privacy-preserving. When the object of IoT has a certain trust value, it is able to determine which data content can be accessed. The process of trust evaluation is shown in Fig. 1.

(1) Direct interactive trust

In this, we assume that human can judge the validity of the data. We only consider three kinds of interaction behavior, namely the abnormal data, the unauthorized access and the

Manuscript received September 6, 2016.
Manuscript revised October 17, 2016.
Manuscript publicized November 11, 2016.

[†]The author is with School of Computer Science and Engineering, Northeastern University, Shenyang 110819, China.
[††]The author is with Hebei Engineering Technology Research Center for IOT Data acquisition & Processing, North China Institute of Science and Technology, East Yanjiao, Beijing 101601, China.
a) E-mail: zhenguo@126.com
b) E-mail: tianliqin@ncist.edu.cn

DOI: 10.1587/transinf.2016EDL8185

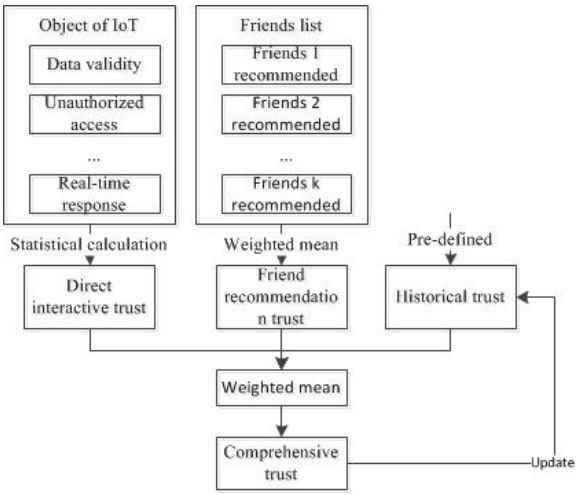

Fig. 1 Process of trust evaluation.

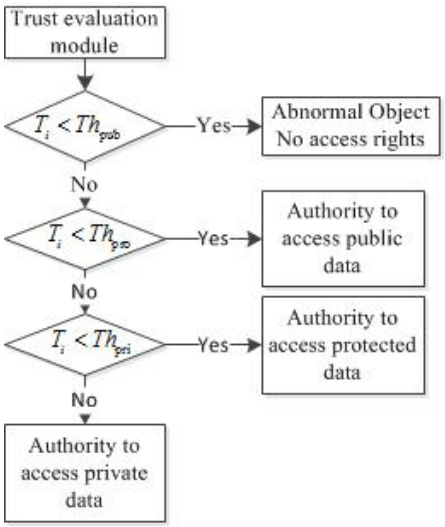

Fig. 2 The process of access control.

abnormal response.

Direct interactive trust is calculated at the end of the interaction, so when the interaction begins to determine the access, the value of direct interactive trust is equal to the value of historical trust.

The total number of communication between the i-th object and human is denoted as m. The invalid data's number of the i-th object is denoted as m_d. The number of unauthorized access is denoted as m_u. The number of non-real time response is denoted as m_{nr}. The direct interactive trust of the i-th object is recorded as T_i^{dit}. Then the calculation method is shown in the formula 1.

$$T_i^{dit} = \lceil MAX \times ((3 - (m_d + m_u + m_{nr})/m)/3) \rceil \tag{1}$$

Where MAX is a maximum value and it is pre-defined.

(2) Friend recommendation trust

Each human will save a friends list. So each human can get a trust value of the i-th object from his friends. We assume that this person has n friends, of which k friends have a trust evaluation of the i-th object. The comprehensive trust of the i-th object provided by the j-th friend is recorded as T_i^j. The friend recommendation trust of the i-th object is recorded as T_i^{frt}. Then the calculation method is shown in the formula 2.

$$T_i^{frt} = \begin{cases} \left| \sum_{j=1}^{k} \left(\frac{T_i^j}{k} \right) \right|, & 0 < k \le n \\ MAX, & k = 0 \end{cases} \tag{2}$$

(3) Historical trust

We introduce three thresholds, namely the public threshold (recorded as Th_{pub}), the protected threshold (recorded as Th_{pro}) and the private threshold (recorded as Th_{pri}) satisfying $0 < Th_{\text{pub}} < Th_{\text{pro}} < Th_{\text{pri}} < MAX$. The initial value of historical trust is set H ($H \in [Th_{\text{pub}}, Th_{\text{pro}})$) and updated according to data trust. The comprehensive trust of the i-th object is recorded as T_i. The calculation method is shown in the formula 3.

$$T_i^{ht} = \begin{cases} H, & initial \\ T_i, & other \end{cases} \tag{3}$$

(4) Comprehensive trust

The value of comprehensive trust is obtained by the weighted average, using direct interactive trust, friend recommendation trust and historical trust. The calculation method is shown in the formula 4.

$$T_i = \left\lceil \alpha \times T_i^{dit} + \beta \times T_i^{frt} + \gamma \times T_i^{ht} \right\rceil \tag{4}$$

Where α, β, γ are weighting coefficients, and $0 \le \alpha, \beta, \gamma \le 1$, $\alpha + \beta + \gamma = 1$. The user, the experts and the experience can set its value.

The trust value of the first interactive object is set by the human. The general value is greater than the public threshold and less than the protection threshold.

2.2 Privacy Classification Module

The information of human can be classified in three levels, namely, public, protected and private. The criteria and rules of classification are determined by each human. The public information generally does not involve personal privacy and can be accessed by any normal object. The protected information and private information contains the contents of personal privacy and can only be accessed by a particular normal object.

2.3 Access Control Module

The level of the data that an object can access is determined by the trust value and the thresholds of object. The process of access control is shown in Fig. 2.

This indicates the higher the trust value, the more privacy data can be accessed. It also conforms to the social rules of human society.

2.4 Performance Analysis

The cost of trust model was mainly derived from the calculation of T_i^{frt}, its value was $O(k)$. The size of public, protected and private data was recorded as s_1, s_2, s_3 respectively. The communication overhead of objects in IoT was $O(s_1 + s_2 + s_3)$. Due to the limitation of the trust threshold, the actual data in the communication process is much smaller than the total amount of data.

3. Simulation Results and Analysis

In order to analyze the validity of the privacy-preserving model, the model will be carried on verification through a simulation experiment environment.

3.1 Simulation Environment and Parameter Setting

The experiment is carried out to evaluate the performance of algorithm on OMNeT++ platform. We construct a runtime environment that contains 20 objects. Of these objects, 5 of which are human objects. The other 15 are non-human objects of IoT. The position of the human object is moving. And 5 human objects are friends. The exchange of trust between humans is integrated by two mechanisms, the regular exchange and the trigger exchange. In this way, we can ensure the timely detection of abnormal objects. The parameters of the simulation environment are set as shown in Table 1. The parameters of the trust model are shown in Table 2.

3.2 Simulation and Analysis

(1) Object distribution and topology
In the experiment, the number of objects was 20. Human objects were set to 5. Each interaction has 10 communications. The objects are randomly distributed in a square area. When an interaction is complete, the human object is moved to a new location at random. The value of parameter is shown in Table 1. Figure 3 is a graph of objects distribution and topological graph with 20 objects. Among them, the index 0, 5, 10, 15, 19 is defined as a human object.
(2) The change trend of trust value
In this, taking objects (with index 8) as an example, we analyze the change trend of the object's trust value. The change trend of the object's trust value was shown in Fig. 4.

As can be seen from Fig. 4, direct interaction trust has a relatively large fluctuation because of the impact of interactive behavior. Friends recommend trust, historical trust and comprehensive trust change trends are basically the same. Because of the exchange of trust between the friend and the trigger mechanism, the calculation of the trust value of the object is based on different human objects, but the change trend is basically stable. When there is a exception of direct interaction trust, the trigger mechanism can be timely notification to other friends. The abnormal state of this object can be known by all friends. From the change of the value of trust, the trigger mechanism has reached its effect.
(3) Comparison of energy consumption
Privacy-Preserving model can reduce the content of data access, which can reduce the amount of data in the com-

Table 1 Parameter values of simulation environment.

Parameter	Value	Parameter	Value
Number of Nodes	20	Initial energy of Node	0.2J
Nodes' Distribution	200m×200m	Sim-Time-Limit	200s

Table 2 Parameter values of trust model.

Parameter	Value	Parameter	Value
MAX	100	n	5
$\left(Th_{pub}, Th_{pro}, Th_{pri}\right)$	(50,70,90)	m	10
$\left(\alpha, \beta, \gamma\right)$	(0.3,0.3,0.4)	-	-

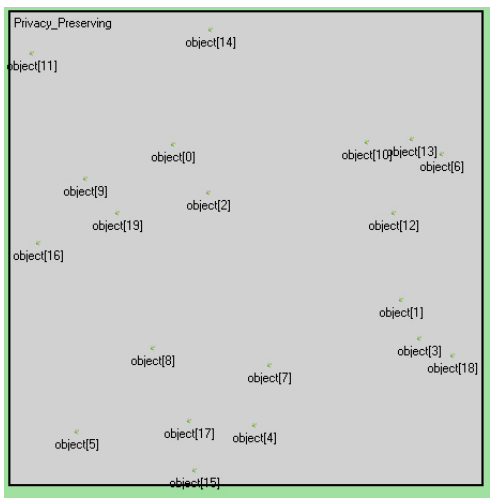

Fig. 3 Objects distribution and topological graph.

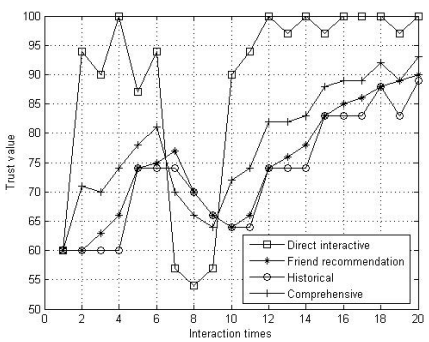

Fig. 4 The change trend of the object's trust value.

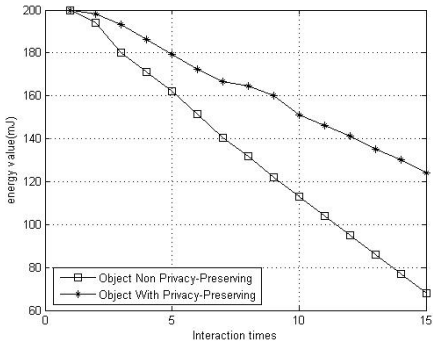

Fig. 5 Comparison of energy consumption.

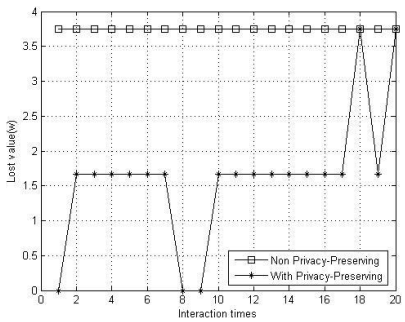

Fig. 6 Comparison of privacy loss.

munication process, and reduce the energy consumption of objects of IoT. The comparison of energy consumption is shown in Fig. 5.

(4) Comparison of privacy loss

Privacy loss is the loss (such as property, etc.) caused by unauthorized access to private information. It is a dummy value in this paper. The basic unit of the privacy loss is *w*. Assuming that the public data access loss is 0, the loss of access to the protected data is 5, and the loss of access to private data is 10. The comparison of privacy loss is shown in Fig. 6.

Figure 6 shows that after the privacy-preserving model is introduced, the loss caused by unauthorized access is greatly reduced.

4. Conclusion

A Privacy-Preserving model of human Interaction with IOT based trust evaluation is proposed. In this model, we use the behavior and data of interaction process and social nature of human to construct the trust evaluation mechanism. The trust mechanism can meet the needs of privacy protection and has good characteristics. For example, trust can be dynamically updated, abnormal can be found in a timely manner, privacy can be effectively protected. The trust value of each interactive object is obtained through the trust mechanism. Given a threshold, the privacy protection problem is transformed into a simple judgment problem. If the trust value satisfies a certain threshold condition, the object can access the privacy data. In order to protect the data more effectively, we divide the data into three levels, which can satisfy the interaction requirements of different trust relationships. In addition, due to the interaction process using trust control, so that the communication reduces data volume, thus saving the energy of object.

Acknowledgments

The work was supported by the National Natural Science Foundation of China (61472137), the Natural Science Foundation of Hebei Province (F2014508028), the Science and technology project of Hebei Province (15210703) and the Fundamental Research Funds for the Central Universities (3142015022). We express our thanks to person who checked our manuscript.

References

[1] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," Computer Networks, vol.57, no.10, pp.2266–2279, 2013.

[2] S. Sicari, A. Rizzardi, L.A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," Computer Networks, vol.76, pp.146–164, 2015.

[3] A. Alcaide, E. Palomar, J. Montero-Castillo, and A. Ribagorda, "Anonymous authentication for privacy-preserving IoT target-driven applications," Computers & Security, vol.37, no.9, pp.111–123, 2013.

[4] L. González-Manzano, J.M. de Fuentes, S. Pastrana, P. Peris-Lopez, and L. Hernández-Encinas, "PAgIoT – Privacy-preserving aggregation protocol for Internet of Things," Journal of Network & Computer Applications, vol.71, pp.59–71, 2016.

[5] I. Chatzigiannakis, A. Vitaletti, and A. Pyrgelis, "A privacy-preserving smart parking system using an IoT elliptic curve based security platform," Computer Communications, vol.89-90, pp.165–177, 2016.

[6] K. Kang, Z.B. Pang, and C. Wang, "Security and privacy mechanism for health internet of things," Journal of China Universities of Posts & Telecommunications, vol.20, no.13, pp.64–68, 2013.

[7] B. Zhang, C.H. Liu, J. Lu, Z. Song, Z. Ren, J. Ma, and W. Wang, "Privacy-preserving QoI-aware participant coordination for mobile crowdsourcing," Computer Networks, vol.101, pp.29–41, 2016.