Mathematical Biosciences and Engineering

MBE, 18(4): 3977–3992.
DOI: 10.3934/mbe.2021199
Received: 06 March 2021
Accepted: 28 April 2021
Published: 07 May 2021

http://www.aimspress.com/journal/MBE

Research article

Research on multi decision making security performance of IoT identity resolution server based on AHP

Huqing Wang [1,2,*] and Zhixin Sun [1,2]

[1] Technology Research and Development Center of Postal Industry of State Post Bureau, Nanjing University of Posts and Telecommunications, Nanjing 210003, China
[2] School of Modern Posts, Nanjing University of Posts and Telecommunications, Nanjing 210003, China

* **Correspondence:** Email: wanghuqing@njupt.edu.cn.

Abstract: The application scenarios of IoT (Internet of Things) are complex and diverse. Failure of security defense in any part of IoT can lead to huge information leakage and incalculable losses. IoT security issues are affecting and limiting its application prospects, and have become one of the hotspots in the field of IoT. Identity resolution security of IoT has become a core issue in solving the security problem of IoT. The aim of this paper is to apply AHP, a well-known decision making method, to IoT identity resolution security. Selecting 6 indicators, several pairwise comparison matrices are constructed based on scores from experts and lab researchers. The AHP method is used to calculate malicious resolution value as a quantitative basis for judging the security performance of each resolution server. An experimental case is used to verify the validity and correctness of the AHP-based IoT identity resolution security evaluation model.

Keywords: IoT identity resolution; IoT addressing; AHP; IoT security

1. Introduction

The Internet of Things (IoT) breaks away from the traditional communication mode between people. It introduces perception of the physical world. It establishes the communication between people and things, between things and things, enabling dynamic collection, intelligent processing, seamless interaction and collaborative sharing of information. The “things” in IoT include the objects in the physical world and information world. These objects can be integrated into the communication network by being identified. In order to interconnect all things in the IoT, all these kinds of things must

be effectively and uniquely identified. Through identification, the physical or logical entity object in IoT can be uniquely identified within a specified range and enable the query, management and control of the entity information can be realized. Object identification provides the basis for a variety of IoT applications. With the identity of objects, mapping the object name to the address of a server that stores the information enables the viewing the object details. Identity and mapping can be referred to as the identity and resolution mechanism of IoT [1].

IoT is characterized by mass communication. A large number of things exchange information every moment in the IoT. Identity resolution technology is a key technology to enable global information about things to be queried, located, managed and circulated across domains. During these above process, many sensitive information such as products, manufacturers and logistics may be involved [2]. Competitors or people with ulterior motives can intercept identity resolution information to gain access to trade secrets such as production and profits of goods manufacturers. Some pranksters may also deliberately tamper with the identity resolution information, resulting in substantial financial losses and disputes. The security protection of identity resolution is very important. Only the security problem of identity resolution of IoT is guaranteed, can IoT really play a role in various application fields. According to a survey of more than 5000 enterprises around the world, the top three barriers to the deployment of IoT are data security and privacy, integration with existing IT systems, and cases of lack of persuasion. The gap between the demand side and the supply side will be an important problem to be solved in the future development of IoT industry [3].

At present, most of the researches of the identity resolution technology have focused on discussing the compatibility and efficiency of resolution procedure. There has been little new research on the security aspects of identity resolution. Some common security methods in Internet, such as identity authentication, digital signature, encrypted transmission, etc. have been adopted in the field of IoT identity resolution. These common strategies can enhance the security of identity resolution to a certain extent. However, the above security measures involve issues such as the cost of encryption mechanism, key management, anti-flow-attacks and other issues and do not take into account the special characteristics of the IoT, such as the interconnection of a large number of goods. Moreover, the identity resolution of IoT is a multi-level recursive parsing technology. The security architecture is complex and the security field covers a wide range of areas. The processing capacity of terminal devices or apparatuses connected to IoT is very different. They interaction among them and the trust relationships are complex. Therefore, it is necessary to consider the security issues of differentiated systems. Even if some security measures in Internet guarantee the security of individual resolution levels, they cannot guarantee the overall security of identity resolution in IoT, because IoT is a large system integrating multiple levels, and many security problems come from system integration.

The security of identity resolution of IoT has become a core issue in solving IoT security problems, and it is also a major technical problem. The emphasis of our study lies in establishing a comprehensive and effective security evaluation system for identity resolution that can be applied to all levels. Based on the advantages of Analytic Hierarchy Process (AHP) in solving complex multi-objective decision-making problems, combined with the influencing factors of identity resolution security, this paper proposes an AHP-based security evaluation model of the IoT. The security influencing factors of identity resolution are first investigated, and then industry experts and front-line laboratory researchers are invited to score the influencing factors and the past behavior of each resolution server. One mathematical model based on AHP is established to obtain the comprehensive evaluation score of each resolution server. With AHP model, the qualitative problem is transformed into a quantitative problem.

Through the comprehensive evaluation score, the resolution safety factor of each resolution server can be displayed intuitively, and the judgement basis for the user's trust degree of the resolution server can be made.

The remainder of this paper is consists of the following sections. Section 2 investigates the current security technology of IoT identity resolution. Section 3 first describes the Analytic Hierarchy Process (AHP), and then applies AHP to the security evaluation model of IoT identity resolution. Section 4 shows one case analysis. Finally, we conclude this paper and propose future work in section 5.

2. Related work

This section discusses the related work in the field of identity resolution security. The standardization organizations related to IoT are actively promoting the research of goods identity resolution technology, which leads to the current coexistence of various identity resolution systems. There are a variety of IoT identity resolution systems available at home and abroad, which can be divided into two categories: improved identity resolution system based on Domain Name System (DNS) and innovative identity resolution system independent of DNS [4]. IoT is an extension of Internet. Years of Internet practice has proven the success of DNS resolution system. Therefore, an improved DNS-based resolution scheme is the preferred choice for the IoT. For example, the Electronic Produce Code (EPC) technology proposed by MIT [5], Object Identifier (OID) technology jointly developed by ISO/IEC and ITU-T [6,7], entity code for IoT (Ecode for IoT) used in China [8]. Like most Internet protocols, DNS is designed with security vulnerabilities. DNS is the core of Internet, which makes it an important target for attackers. DNS resolution is implemented by domain name server, especially relying on root domain name server. It is a centralized architecture. There are problems such as central structure failure, load imbalance and over reliance on central trust [9]. At the same time, IoT involves a large amount of sensitive information including products, manufacturers and logistics, which brings higher privacy protection requirements. Due to the loopholes in its architecture, there are cache snooping, domain name hijacking, DNS spoofing, denial of service (DoS) and other security threats during DNS resolution process. User's privacy information is easily disclosed and DNS resolution record is easily changed. These seriously affect the network service quality. The main solution to the security problem of the improved DNS resolution system is to use the common security means such as identity authentication, digital signature, encrypted transmission, DNSSEC and DNSCurve in Internet [10], which can enhance the confidentiality of goods identity resolution to a certain extent. These means can prevent the resolution data from being intercepted by attackers to gain access to the user's private information. But, the cost of security means is also high. We need to consider the characteristics of the limited resources of IoT for further research.

The innovative DNS-independent identity resolution system consists mainly of Handle, UID, and the emerging blockchain resolution technology in recent years. Handle system sets one or more administrators for each handle ID. Administrators need authentication and authority authentication before responding to any handle management request. Similarly, when the client initiates a resolution request, authentication is also required. Handle architecture designs a new application layer resolution and security protection scheme, but its identity authentication method is still realized by the traditional private key signature technology [11]. UID is a kind of environment aware technology for ubiquitous computing [12]. It identifies physical or logical objects such as objective entities, spaces, addresses, concepts, through ubiquitous codes (ucode). UID resolution system divides the security and privacy

protection requirements into 7 levels to achieve differentiated security services for different applications. However, the traditional security protection technology is also used in the specific implementation. Besides, UID system is mainly used in the project of Tron (the real-time operating system nucleus) in Japan, and it is only used in some application scenarios.

In recent years, some scholars have applied the popular blockchain technology to the identity resolution. Blockchain, as a novel decentralized solution, can provide innovative ideas for flattening the DNS architecture and realizing a co-management model between global domain names service providers. Namecoin [13] is the first domain name system to realize decentralization. The cost of Namecoin is low, but it cannot prevent illegal occupation, resulting in a large number of Botnet domain names. Therefore, the domain name space is very poorly utilized. Besides, the system would be insecure if more than 60% of the computing power controlled a mining pool [14]. Namecoin enables decentralized domain name registration and distribution, which leads to the problem of domain name preemption and the lack of dispute resolution mechanism. Namecoin is difficult to be compatible with current DNS. Blockstack [15] ameliorates the security problem associated with low Namecoin node activity and is built directly on the bitcoin blockchain system. Blockstack embeds domain name data into special fields of bitcoin transaction records. With the security of the Bitcoin blockchain's network environment. Blockstack identifies and analyzes the domain name information in the new block, and realizes the establishment of a virtual domain name data link on the host blockchain [16]. Blockstack also has some problems. First of all, the technology is based on bitcoin and uses the PoW consensus algorithm. The mining capacity and transaction flow in bitcoin are still centralized, with 51% attack threat [17]. In addition, PoW is susceptible to forking, leading to inconsistent data [18]. Handshake [19] is a public chain scheme based on UTXO model. It replaces the fully trusted registration authority in DNS system and uses decentralized trust anchor to prove domain ownership. Trust anchor is composed of decentralized blockchain and incentive mechanism. It optimizes the decentralization, cooperates with the association consensus between domain name and certificate, and no longer relies on a single trusted institution. The above three schemes are innovative attempts in the application of blockchian under the identity resolution, which have opened up new ideas and new horizons [20]. However, the current research on blockchain in identity resolution is mostly academic discussion and theoretical analysis, lacking practical cases [21,22].

The above overview study shows that the secure identity resolution method of IoT has become a very important security factor in the application of IoT. The existing solutions for the security resolution of IoT mainly have the following problems: 1)focus on the resolution security of each layer, while ignoring the integrated security of the whole resolution architecture of IoT; 2) use the traditional Internet security solutions, ignoring the particularity of IoT; 3) these methods can provide some security measures during the resolution process, but it is difficult to judge the security performance of the resolution server; 4) the research of emerging technologies such as blockchain is still at the primary stage of theoretical research, which is far from the practical application. The security problem of IoT identity resolution has become a technical problem. The quantitative and comprehensive evaluation of resolution security is of considerable importance towards the resolution server in IoT. In this paper, the area of identity resolution security is taken as the main research subject and an AHP-based security evaluation model is proposed. The construction of this model is described specifically in the following sections.

3. Security evaluation model of IoT identity resolution based on AHP

3.1. Introduction to AHP

The AHP is a decision-making method developed and used by the American operations research expert T. L. Saaty in the mid-1970s. It is usually used to solve complex multi-objective decision-making problems with a combination of qualitative and quantitative analysis [23]. The main idea is to treat a complex multi-objective decision-making problem as a system, decomposing the objective into multiple objectives or criteria, if necessary, further decomposing it into sever levels including multi-level sub indicators, calculating the hierarchical single ranking and total ranking through the fuzzy quantitative method of qualitative indicators, and making decisions according to the ranking results. AHP makes use of the characteristics of behavior science to quantify empirical judgments of decision makers. It is suitable for the situation where the structure of the objectives is complex and the necessary data is lacking. It is common tool for mathematical analysis in system science.

AHP can transform complex and ambiguous correlation into quantitative analysis problems and effectively measure the judgment and comparison of decision makers. It is widely used in social, economic, management and other application fields [24,25]. For example, it can be used in the context of graduate employment problems. Both graduates and employers have their own selection criteria and requirements. For graduates, the relevant criteria include: matching degree of job position and specialty, higher income, a good living environment, a good reputation of the company, a good working environment, and more opportunities for future development, etc. Among those criteria, a good living environment can be divided into some molecular criteria, such as big cities and climate conditions. When a graduate is faced with a variety of choices and decisions, AHP method can be used to quantify the above criteria. The quantitative value of each optional company is calculated by weighting, and the decision can be made according to the result of ranking.

There are many kinds and a large number of devices in IoT. These devices are easily exposed and vulnerable to security threats. To judge and select an identity resolution server with high security performance, there are many evaluation indicators, such as resolution efficiency, ease of operation, integrity of resolution results, malicious resolution behavior, etc., which also belong to a multi-objective decision-making problem. When evaluating the security performance of a resolution server, we can quantify these evaluation criteria and historical resolution behavior, and then apply AHP method to establish a hierarchical evaluation model to calculate the security performance evaluation score of the resolution server.

3.2. Design idea of security evaluation model of IoT identity resolution

In this paper, a security evaluation model for IoT identity resolution based on the AHP method is proposed. The design idea of this model is shown in Figure 1 below.

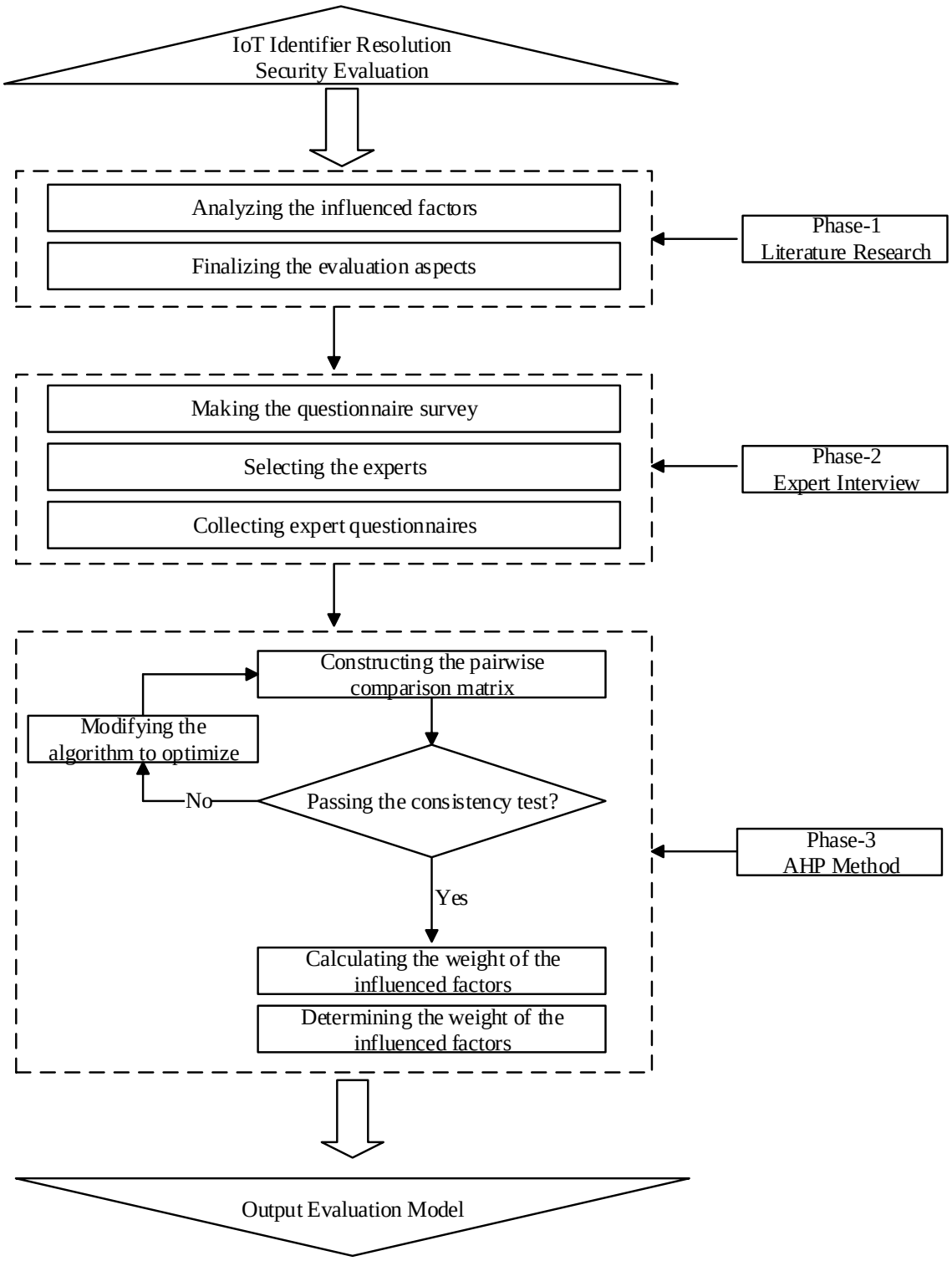

Figure 1. Design idea of the security evaluation model of IoT identity resolution.

This security evaluation model is divided into the following 3 phases.

In phase-1, based on the research of other scholars and combined with the authors' work experience, the relevant factors affecting the security evaluation mechanism of IoT identity resolution are discussed, and the evaluation indicators are selected according to the impact degree. The evaluation indicators are the basis of comprehensive evaluation research, and its rationality and

comprehensiveness directly affect the results of evaluation studies.

In phase-2, industry experts and relevant laboratory researchers are invited to score the evaluation indicators and quantify the pairwise comparison value of each resolution server under each indicator. According to the score, the indicators judgment matrix and pairwise comparison matrix are constructed. The rationality of expert scoring and the scale of judgment matrix have an important impact on the establishment of the security evaluation model of IoT identity resolution. The experts invited in this paper are not only front-line lab researchers from the IoT industry for many years, but also the scientific experts in this field. They can effectively judge the security of the resolution server, reasonably score the impact indicators. Their expertise and industry experience qualify for the construction conditions of judgment matrix. According to the principle of AHP, the judgment matrix adopts the scale of 1–9, and the lager the number, the higher the importance.

In phase-3, AHP is used to calculate the weight vector of each evaluation indicator. Firstly, the score of all experts is processed by arithmetic mean. Then the maximum eigenvalue and eigenvector of the matrix are calculated, and the maximum eigenvalue is used for consistency checking. If it fails to pass the consistency check, the optimization algorithm is selected to continue processing the matrix value. It is important to note that there is a certain subjectivity in the selection and scoring of experts, which leads to the probability that the construction matrix cannot pass the consistency check. This result affects the application of AHP. At this time, it is necessary to go back to the phase-1 or phase-2, reconsider the selection of evaluation indicators or reply to the experts with the feedback results and implement a new round of scoring operation. After the comparison construction matrix has passed the consistency check, the data is standardized and normalized, and the weight vector of each indicator is calculated. Based on the comparison construction matrix of all resolution servers under each indicator, a combined weight vector of each resolution server is calculated. According to the total score ranking, the maliciousness of all resolution server can be judged, and the correct decision can be made.

3.3. Model description and definition

3.3.1. Definition of the security evaluation model

Definition 1 (security evaluation model of IoT identity resolution) IIRSEM= {IIRSO, IIRSC, IIRSP}

(1) IIRSO (IoT Identity Resolution Security Objective layer), refers to make quantitative evaluation value for the security performance of IoT identity resolution server.

(2) IIRSC (IoT Identity Resolution Security Criteria layer), refers to the security evaluation indicators that affect the identity resolution server of IoT.

(3) IIRSP (IoT Identity Resolution Security Plan layer), refers to the IoT identity resolution servers.

Using the above security evaluation model of IoT identity resolution, we can quickly and effectively build a security evaluation scenario of identity resolution in IoT application field of mass devices, and then accurately evaluate the security performance and resolution efficiency of the resolution server based on the following evaluation methods, so as to promote the application security of IoT.

3.3.2. Specific steps of the security evaluation model

AHP method is used to evaluate the security of the identity resolution of IoT, including the following steps:

(1) Constructing the 3-level evaluation model

Based on the definition of the above model, a 3-level evaluation model IIRSEM= {IIRSO, IIRSC, IIRSP} is constructed, as shown in Figure 2.

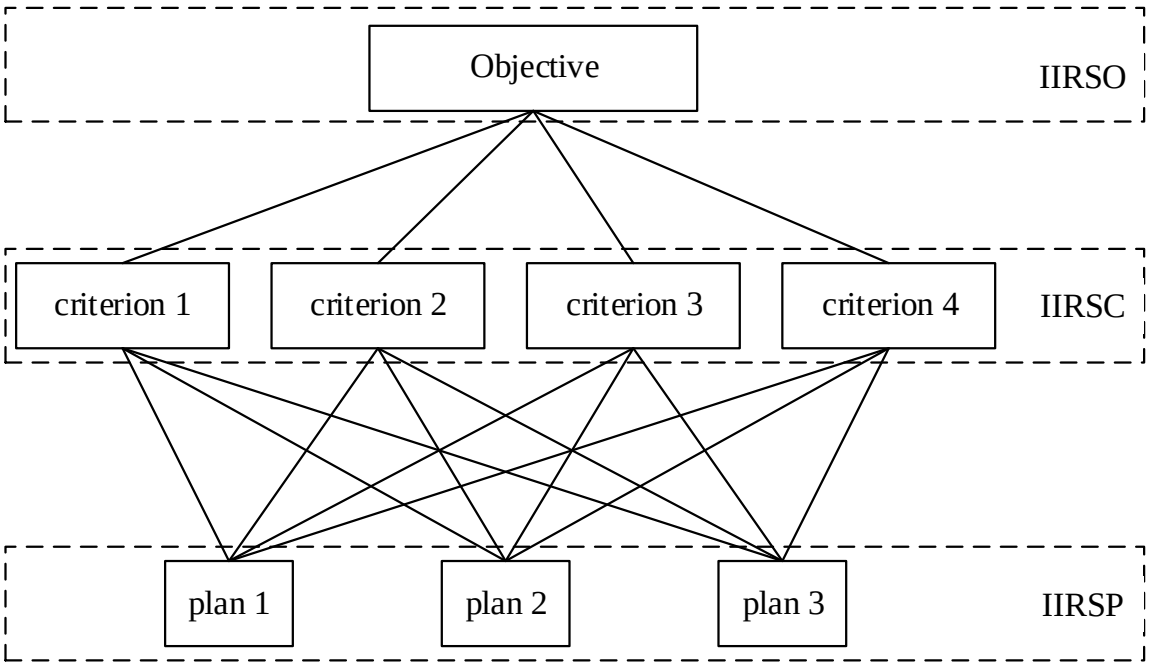

Figure 2. 3-Level Evaluation Model.

IIRSO layer: this layer has only one element, which represents the expected goal or desired outcome of the model. In our model, it is the security evaluation mechanism of IoT identity resolution.

IIRSC layer: this layer includes the intermediate links involved in the realization of objective, and it can consist of multiple layers, including the criteria and sub criteria to be considered. There is no limit to the number of sub-criteria layers, which is related to the complexity of the problem and the degree of detail to be analyzed. On the basis of analyzing the research results of relevant scholars and combining with the previous work experience, this paper summarizes and refines the criteria layer from the two dimensions of the trust degree of the resolution server and the user experience. The evaluation factors affecting the security of IoT identity resolution are shown in figure 3 below. Among them, the trust dimension of resolution server includes historical trust, missing resolution rate and malicious resolution rate. The perceived dimension of user experience includes average resolution latency, ease of identity resolution and integrity of resolution result. It is worth noting that the above dimensions and indicators can be added, modified or removed according to the actual situation to achieve better application resilience.

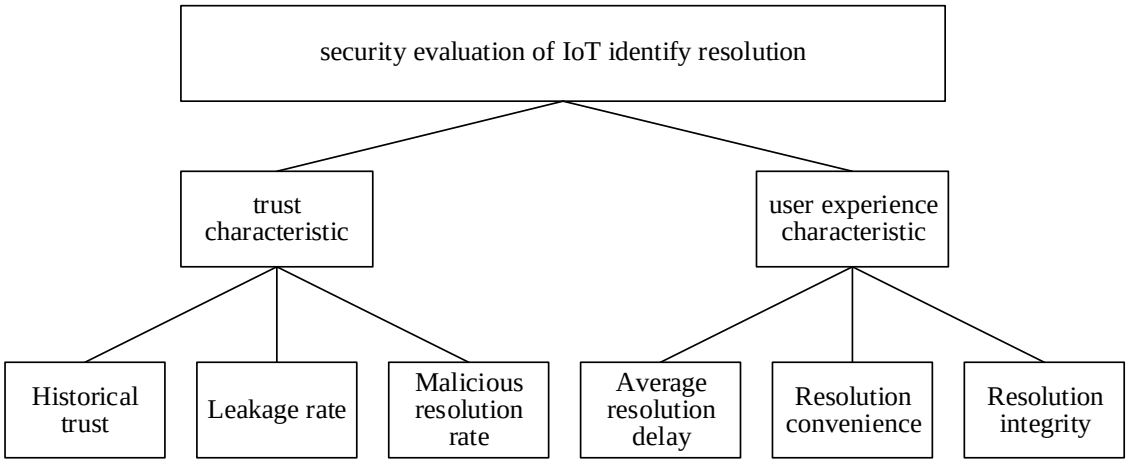

Figure 3. Indicators of the security evaluation model.

IIRSP layer: this layer includes various measures and decision-making schemes to achieve the goal. In our model, it represents multiple resolution servers that can provide identity resolution services.

(2) Constructing the indicator weight pairwise comparison matrix

The pairwise comparison matrix is used to compare the impact of each indicator on the target. This is an important step and is the beginning of the transformation from qualitative to quantitative. The main difficulty in determining the proportion of each indicator's impact on the target is that these proportions are not easy to quantify. They occupy a certain proportion of each decision maker's mind. Santy et al. proposed the method of consistent matrix:

① The method of comparing the indicators in pairs is used, instead of comparing them together.

② The relative scale is used to reduce the difficulty of comparing different indicators and improve the accuracy.

The weight comparison matrix for each indicator is represented by the matrix $K = （k_{ij}）_{m\times m}$, with m being the number of indicators. Matrix K has the following characteristics:

①$k_{ij} > 0$

②$k_{ij} = \frac{1}{k_{ji}}$

③$k_{ii} = 1$

（3）Establishing the pairwise comparison matrix of all plans based on each indicator.

In the same way, for each indicator, pairwise comparison method is used to establish the weight quantization matrix of all plans, which is represented by matrix $C_l = （c_{ij}）_{n\times n}$, n is the number of plans, $l = 1，2，\cdots m$. Similarly, m is the number of indicators. The matrix C_l has the same characteristics as the matrix K above.

(4) Consistency checking of all pairwise comparison matrices

Definition 2: In a pairwise comparison matrix, property

$a_{ij} = \frac{a_j}{a_k} \cdot \frac{a_k}{a_j} = a_{ik} \cdot a_{kj}$ is called the consistency of the matrix.

The various pairwise comparison matrices are subjectively proposed by experienced experts and are susceptible to inconsistent contradictions due to complex factors. N-dimensional pairwise comparison matrices are tested for consistency as follows:

Calculating the consistency index $C.I = \frac{\lambda_{max}-n}{n-1}$, λ_{max} is the largest eigenvalue.

The following table was consulted to obtain AHP average random consistency index $R.I$.

Table 1. AHP average random consistency index.

Order n	R.I
1	0
2	0
3	0.52
4	0.89
5	1.12
6	1.26
7	1.36
8	1.41
9	1.46
10	1.49
11	1.52
12	1.54
13	1.56
14	1.58
15	1.59

According to the formula $C.R = \frac{C.I}{R.I}$, calculating the consistency ratio $C.R$

If $C.R \leq 0.1$, the consistency detection of pairwise comparison matrix is passed, and the matrix can be accepted. Otherwise, some optimization algorithm is selected to modify the matrix or reconstruct the matrix.

(5) Computing the weight vector of all pairwise comparison matrices

Calculate maximum eigenvalues and eigenvectors for each pair of comparison matrices, including the pairwise comparison matrices for the indicators and the pairwise comparison matrices of all plans based on each indicator. The normalized eigenvectors are called weight vectors. The weight vector of the indicator pairwise comparison matrix shows the relative importance of each indicator. The weight vector of the pairwise comparison matrix of all plans based on each indicator shows the score of each plan in terms of the indicator.

(6) Calculating the combined weight vector of each plan

Combining with the weight vector of the indicator comparison matrix, we calculate the combination weight of plan level to criterion level. We can use the result of combination weight vector as the quantitative basis of decision-making.

4. Case analysis

In this section, an experimental case is used to verify the validity and correctness of the AHP-based security evaluation model for IoT identity resolution. In the experimental case, three identity resolution servers are selected for security evaluation and the evaluation indicator of the criteria level includes two dimensions and six influencing factors.

The specific steps are as follows.

Step 1: Constructing the pairwise comparison matrix

The author's team has been studying IoT for more than 10 years, and has made some achievements in IoT industry. The team has more than ten professors, associate professors and doctoral student. In this case, a total of 15 laboratory researchers, experts and scholars from the IoT industry were invited to score. 10 of them are members of our team, and the other 5 are experts from IoT industry outside our team. They also have extensive research experience in IoT field, are involved in the identity resolution in IoT in their work, and attached great importance to the identity resolution security of IoT. After processing the data of 15 questionnaires with arithmetic average, the pairwise comparison matrix Matrix_I of 6 indicators $\{F_i, i = 1{\sim}6\}$ were obtained, as shown in Figure 4 below. The order of 6 indicators $\{F_i, i = 1{\sim}6\}$ in row and column is as follows: historical trust, leakage rate, malicious resolution rate, average resolution latency, resolution ease and resolution integrity. For example, the value $i_{13} = 1/9$ in the first row and third column of Matrix_I indicates that the importance of historical trust in evaluating malicious resolution server is 1/9 of that of malicious resolution rate, in other words, the former is far less important than the latter.

$$\begin{bmatrix} & \mathrm{F}_1 & \mathrm{F}_2 & \mathrm{F}_3 & \mathrm{F}_4 & \mathrm{F}_5 & \mathrm{F}_6 \\ \mathrm{F}_1 & 1 & \frac{1}{7} & \frac{1}{9} & \frac{1}{4} & \frac{1}{4} & \frac{1}{7} \\ \mathrm{F}_2 & 7 & 1 & \frac{1}{6} & 1 & 2 & 2 \\ \mathrm{F}_3 & 9 & 6 & 1 & 6 & 7 & 5 \\ \mathrm{F}_4 & 4 & 1 & \frac{1}{6} & 1 & 1 & \frac{1}{2} \\ \mathrm{F}_5 & 4 & \frac{1}{2} & \frac{1}{7} & 1 & 1 & \frac{1}{3} \\ \mathrm{F}_6 & 7 & \frac{1}{2} & \frac{1}{5} & 2 & 3 & 1 \end{bmatrix}$$

Figure 4. The pairwise comparison matrix Matrix_I.

Step2: Consistency checking

Calculating the maximum eigenvalue of Matrix_I
$\lambda_{max}(Matrix\_I)$=6.3842;
Calculating the consistency index of Matrix_I:

$$\mathrm{C.I}(Matrix\_I) = \frac{\lambda_{max}(Matrix\_I) - n}{n-1} = \frac{6.3842 - 6}{6-1} = 0.0768$$

Calculating the consistency ratio:

$$\text{C. R}(Matrix\_I) = \frac{C.I(Matrix\_I)}{R.I} = \frac{0.0768}{1.26} = 0.061 \leq 0.1$$

Therefore, the pairwise comparison matrix $Matrix\_I$ passed the consistency check.

Step3: Calculating the weight coefficient of all indicators

The eigenvector corresponding to the maximum eigenvalue $\lambda_{max}(Matrix\_I)$ of $Matrix\_I$ is as follows:

$$\{w_1, w_2 \cdots w_6\} = \{0.0449, 0.2517, 0.9146, 0.1541, 0.1247, 0.2425\}$$

The above eigenvector: $w_i' = w_i / \sum_{i=1}^{6} w_i$ is normalized.

Then

$$\{w_1', w_2' \cdots w_6'\} = \{0.026, 0.145, 0.528, 0.089, 0.072, 0.14\}$$

We can derive the weight coefficient of 6 indicators under the two dimensions of resolution server trust value and the user experience, as shown in Figure 5 below.

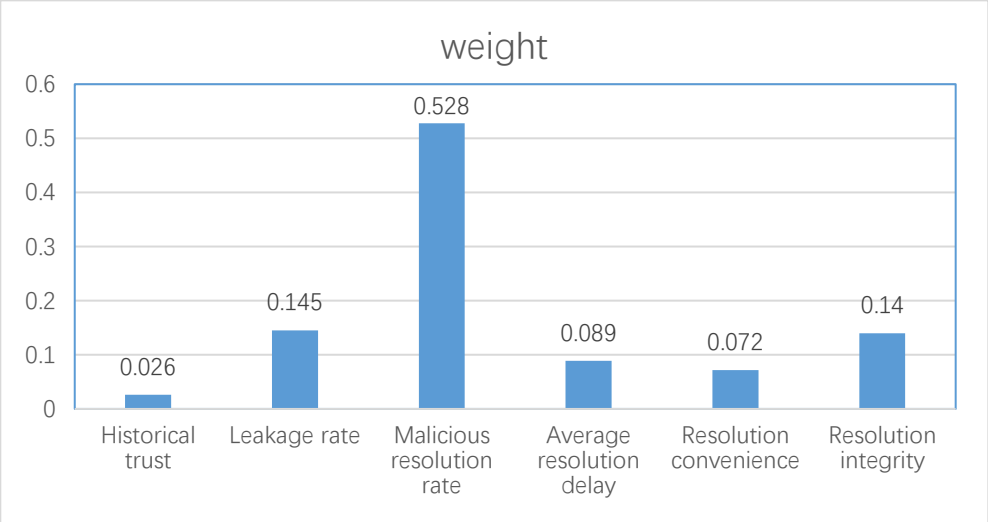

Figure 5. Weight coefficient of 6 indicators.

As can be seen from the figure, the 6 indicators are ranked in order of importance when judging insecure resolution servers: malicious resolution rate, leakage rate, resolution integrity, average resolution latency, ease of resolution, and historical trust.

Step 4: Calculate each plan's score on each indicator

Firstly, according to the experts' scoring, the pairwise comparison matrix of 3 resolution servers $\{IRS_i, i = 1\sim3\}$ in terms of 6 indicators is constructed, as shown in the following figure:

$$\begin{bmatrix} F_1 & \text{IRS}_1 & \text{IRS}_2 & \text{IRS}_3 \\ \text{IRS}_1 & 1 & 6 & 3 \\ \text{IRS}_2 & \frac{1}{6} & 1 & \frac{1}{5} \\ \text{IRS}_3 & \frac{1}{3} & 5 & 1 \end{bmatrix} \quad \begin{bmatrix} F_2 & \text{IRS}_1 & \text{IRS}_2 & \text{IRS}_3 \\ \text{IRS}_1 & 1 & 9 & 3 \\ \text{IRS}_2 & \frac{1}{9} & 1 & \frac{1}{5} \\ \text{IRS}_3 & \frac{1}{3} & 5 & 1 \end{bmatrix}$$

$$\begin{bmatrix} F_3 & \text{IRS}_1 & \text{IRS}_2 & \text{IRS}_3 \\ \text{IRS}_1 & 1 & \frac{1}{7} & \frac{1}{3} \\ \text{IRS}_2 & 7 & 1 & 3 \\ \text{IRS}_3 & 3 & \frac{1}{3} & 1 \end{bmatrix} \quad \begin{bmatrix} F_4 & \text{IRS}_1 & \text{IRS}_2 & \text{IRS}_3 \\ \text{IRS}_1 & 1 & 7 & 3 \\ \text{IRS}_2 & \frac{1}{7} & 1 & \frac{1}{2} \\ \text{IRS}_3 & \frac{1}{3} & 2 & 1 \end{bmatrix}$$

$$\begin{bmatrix} F_5 & \text{IRS}_1 & \text{IRS}_2 & \text{IRS}_3 \\ \text{IRS}_1 & 1 & 7 & 4 \\ \text{IRS}_2 & \frac{1}{7} & 1 & \frac{1}{3} \\ \text{IRS}_3 & \frac{1}{4} & 3 & 1 \end{bmatrix} \quad \begin{bmatrix} F_6 & \text{IRS}_1 & \text{IRS}_2 & \text{IRS}_3 \\ \text{IRS}_1 & 1 & \frac{1}{9} & \frac{1}{5} \\ \text{IRS}_2 & 9 & 1 & 4 \\ \text{IRS}_3 & 5 & \frac{1}{4} & 1 \end{bmatrix}$$

Figure 6. Pairwise comparison matrix of 3 resolution servers in terms of 6 indicators.

Then, step2 and step3 were repeated for each of the six pairwise comparison matrices, performing consistency detection and weight coefficient calculation respectively. Finally, the scores of 3 identity resolution servers in terms of 6 indicators are obtained, as shown in Table 2 below.

Table 2. Scores of 3 identity resolution servers in 6 indicators.

	F1	F2	F3	F4	F5	F6
IRS1	0.635	0.672	0.088	0.682	0.705	0.06
IRS2	0.078	0.063	0.669	0.102	0.084	0.709
IRS3	0.287	0.265	0.243	0.216	0.211	0.231

Step 5: Calculate the comprehensive score of each plan

According to the results of step3 and step4, the comprehensive scores of each plan can be calculated, as shown in Table 3 below.

Table 3. comprehensive scores of each plan.

Indicator	**F1**	**F2**	**F3**	**F4**	**F5**	**F6**	**Comprehensive Score**
Weight Coefficient	0.026	0.145	0.528	0.089	0.072	0.14	
IRS2	0.635	0.672	0.088	0.682	0.705	0.06	0.28
IRS3	0.078	0.063	0.669	0.102	0.084	0.709	0.479
IRS3	0.287	0.265	0.243	0.216	0.211	0.231	0.241

The table above shows that the comprehensive scores of 3 identity resolution servers are ranked as follows: IRS2> IRS1 > IRS3.

That is to say, IRS2 has the highest level of maliciousness in terms of identity resolution security; conversely, IRS3 has the highest security.

Compared to other methods of IoT identity resolution security, our model takes advantage of AHP multi decision quantitative analysis. Six evaluation factors are selected and assigned different weights. According to the score of each evaluation factor of historical resolution behavior, the combined score of three identity resolution server is calculated respectively. Finally, the total score of each resolution server can be obtained quantitatively. The total score is used to determine the security performance of each resolution server. The judgment of the security performance of a resolution server is affected by many factors, and is somewhat subjective, which is in line with the characteristics of AHP model. It is feasible to use AHP model to judge the security performance of resolution server. In our model, a number of industry experts are invited to score the weight of six impact factors. Three resolution servers in our laboratory are selected. The score of the historical resolution behavior is also scored by the front-line experts, which makes the application of the model have a certain practical significance.

5. Conclusion

This paper introduces in detail an AHP-based security evaluation model for IoT identity resolution. The design idea and specific steps of this model are presented. A specific experimental case is conducted to illustrate the performance of the proposed model. The experiment shows that our model has good applicability to a certain extent, and can effectively determine the security performance of the resolution server. Identity resolution security plays an important role in the application security of IoT. The research results of this paper allow for quantitative and comprehensive evaluations of IoT identity resolution security.

Based on our experience and the application scenarios of IoT in our laboratory, we select six indicators to evaluate the security of resolution server. The weight of the influence factors and the scoring of the historical resolution behavior of the three resolution servers are mainly given by the experts in our team. The above behaviors are subjective, which is where the defect of our model lie. In the future, this model can be extended to a wider range of IoT applications, and other evaluation indicators can be considered according to the actual application. When using AHP is used to determine the weight, it is necessary to collect more opinions from relevant researchers and experts to make the calculated weight more realistic and to maximize the applicability of the model. In addition, the methods to improve the objectivity of the scoring of indicators and the consistency of the paired comparison matrix are also worth studying.

Acknowledgments

This research was supported by the National Natural Science Foundation of China under Grant (No. 61972208), the project of Nanjing University of Posts and Telecommunications (No.NY219119).

Conflict of interest

All authors declare no conflicts of interest in this paper.

References

1. P. Q. Wang, H. Luo, Y. Sun, Mapping model of multi-identifiers oriented to Internet of Things, *Sci. China Inform. Sci.*, **43** (2013), 1244–1264.
2. Y. J. Xia, W. Z. Chen, X. J. Liu, L. M. Zhang, X. L. Li, Y. Xiang, Adaptive multimedia data forwarding for privacy preservation in vehicular ad-hoc networks, *IEEE Trans. Intell. Transp. Syst.*, **99** (2017), 1–13.
3. China Academy of Information and Communications Technology, *White Paper on Internet of Things*, 2018.
4. Y. Z. Ren, R. C. Xie, S. Q. Zeng, H. R. Zhao, J. Y. Yu, R. Huo, et al., Survey of identity resolution system in industrial Internet of things, *J. Commun.*, **40** (2019), 138–155.
5. EPCglobal, The EPCglobal architecture framework, *The EPCglobal Standards Development Process*, 2007.
6. ISO/IEC, Information technology—open systems interconnection—part1: Object identifier resolution system, *ISO/IEC29168-1,* 2011.
7. ISO/IEC, Information technology—open systems interconnection—part2: Object identifier resolution system, *ISO/IEC29168-2,* 2011.
8. National Standardization Administration of China, Identification system for Internet of things—Ecode resolution specification, *GB/T 36605-2018*, 2018.
9. Mark Allman, Comments on DNS robustness, *ACM, Proceedings of the Internet Measurement Conference 2018, (IMC 2018),* 84–90.
10. K. Chetioui, G. Orhanou, S. Hajji, New protocol E-DNSSEC to enhance DNSSEC security, *Int. J. Net. Secur*., **20** (2018), 19–24.
11. S. Sun, S. Reilly, L. Lannom, Handle system namespace and service definition, *RFC 3651*, IETF, 2003.
12. UID Center, Ubiquitous code, *ucode,* 2009.
13. C. Grothoff, M. Wachs, M. Ermert, J. Appelbaum, Toward secure name resolution on the internet, *Comput. Secur.,* **77** (2018), 694–708.
14. G. B. He, W. Su, S. Gao, J. R. Yue, TD-Root: A trustworthy decentralized DNS root management architecture based on permissioned blockchain, *Future Gener. Comput. Syst.,* **102** (2020), 912–924.
15. T. Takayanag, Y. Kurose, T. Harada, Hierarchical task planning from object goal state for human-assist robot, *2019 IEEE 15th International Conference on Automation Service and Engineering*, (2019), 1359–1366.
16. A. S. Konoplev, A. G. Busygin, D. P. Zegahda, A blockchain decentralized public key infrastructure model, *Autom. Control Comput. Sci.*, **52** (2018), 1017–1021.
17. A. Narayanan, J. Bonneau, E. Felten, A. Miller, S. Goldfeder, Bitcoin and cryptocurrency technologies: A comprehensive introduction, *Princeton University Press*, 2016.
18. X. Q. Li, P. Jiang, T. Chen, X. P. Luo, Q. Y. Wen, A survey on the security of blockchain systems, *Future Gener. Comput. Syst.,* **107** (2020), 841–853.
19. Handshake project [EB/OL], *https://www.handshake.org*, Access time: 2020-02-14.
20. E. Karaarslan, E. Adiguzel, Blockchain based DNS and PKI solutions, *IEEE Commun. Standards Mag.,* **2** (2018), 52–57.
21. A. Sheikh, V. Kamuni, A. Urooj, S. Wagh, N. Singh, D. Patel, Secured energy trading using Byzantine-based blockchain consensus, *IEEE Access*, **8** (2020), 8554–8571.

22. C. Patsakis, F. Casino, Hydras and IPFS: a decentralized playground for malware, *Int. J. Inform. Secur.*, **18** (2019), 787–799.
23. W. Pedrycz, M. Song, Analytic hierarchy process (AHP) in group decision making and its optimization with an allocation of information granularity, *IEEE Trans. Fuzzy Syst.,* **19** (2011), 527–539.
24. U. Dayanaddan, V. Kalimuthu, Software architectural quality assessment model for security analysis using fuzzy analytical hierarchy process (FAHP) method, *3D Res.*, **9** (2018), 1–10.
25. L. Fang, P. Witold, X. W. Liu, Flexibility degree of fuzzy numbers and its implication to a group-decision-making model, *IEEE Trans. Cybern.*, **49** (2019), 4054–4065.

AIMS Press