Computers, Materials & Continua CMC, vol.65, no.1, pp.683-704, 2020

Comprehensive Information Security Evaluation Model Based on Multi-Level Decomposition Feedback for IoT

Jinxin Zuo[1, 3], Yueming Lu[1, 3, *], Hui Gao[2, 3], Ruohan Cao[2, 3], Ziyv Guo[2, 3] and Jim Feng[4]

Abstract: The development of the Internet of Things (IoT) calls for a comprehensive information security evaluation framework to quantitatively measure the safety score and risk (S&R) value of the network urgently. In this paper, we summarize the architecture and vulnerability in IoT and propose a comprehensive information security evaluation model based on multi-level decomposition feedback. The evaluation model provides an idea for information security evaluation of IoT and guides the security decision maker for dynamic protection. Firstly, we establish an overall evaluation indicator system that includes four primary indicators of threat information, asset, vulnerability, and management, respectively. It also includes eleven secondary indicators of system protection rate, attack detection rate, confidentiality, availability, controllability, identifiability, number of vulnerabilities, vulnerability hazard level, staff organization, enterprise grading and service continuity, respectively. Then, we build the core algorithm to enable the evaluation model, wherein a novel weighting technique is developed and a quantitative method is proposed to measure the S&R value. Moreover, in order to better supervise the performance of the proposed evaluation model, we present four novel indicators includes residual risk, continuous conformity of residual risk, head-to-tail consistency and decrease ratio, respectively. Simulation results show the advantages of the proposed model in the evaluation of information security for IoT.

Keywords: IoT, information security quantitative evaluation, safety score, residual risk.

1 Introduction

With the large-scale deployment and application of Internet of Things (IoT) [Sun, Cai, Li et al. (2018); Lin, Zhou, An et al. (2018); Lin, Zhou, You et al. (2019); Hui, Zhou, Xu et al. (2020);

[1] School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing, 100876, China.

[2] School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing, 100876, China.

[3] Key Laboratory of Trustworthy Distributed Computing and Service (BUPT), Ministry of Education, Beijing, 100876, China.

[4] Amphenol Global Interconnect Systems, San Jose, CA 95131, USA.

[*] Corresponding Author: Yueming Lu. Email: ymlu@bupt.edu.cn.

Received: 30 March 2020; Accepted: 29 May 2020.

Wang, Kong, Guan et al. (2019); He, Xie, Xie et al. (2019)], there are many emerging challenges and issues. In particular, the security and privacy issues are now attracting more attention from both academia and industries [Zhou, Jia, Peng et al. (2019); Wang, Kong, Li et al. (2019); Su, Lin, Zhou et al. (2015); Medhane, Sangaiah, Hossain et al. (2020)]. It is reported that the newly connected IoT terminals will encounter an attempted cyber-attack every five minutes [P. N. Technology (2018)], which indicates that security is still a critical concern to be enhanced. However, there is no standard guidance on the security evaluation methods nor comprehensive regulation for systems and devices of the IoT.

Currently, the information security standards include common criteria (CC) standards [CCRA (2019)], key infrastructure network security improvement framework proposed by the national institute of standards and technology (NIST) [Huang, Debnath, Iorga et al. (2019)] and China's GB series standards. For management and service, China follows ISO9001 and ISO/IEC27001 standards. These standards propose CC evaluation criteria, and security technical requirements of the gateway in the sensing layer of the internet of things, among others. However, a specific set of information security quantization evaluation models is still missing. The promulgation of many standards has promoted the development of information security evaluation, but the inconsistency caused by many standards has also resulted in some inconvenience during the evaluation process. Moreover, traditional evaluation methods are mostly aimed at static evaluation of information security. Therefore, it is of great significance to provide an evaluation framework and model for the information security evaluation of IoT by integrating numerous evaluation criteria.

1.1 Motivation

To address the information security evaluation issues in IoT, numerous researches target at information security and risk evaluation of IoT. Security strategies can be guided by the results of the evaluation to eradicate risks or reduce risks. The ultimate goal of information risk management and security evaluation is to identify risk and quantify safety [Emanuele, Diego, Gerd et al. (2017); Li, Bi, Chen et al. (2018)]. To establish a measurement model for the safety score and risk (S&R) value in IoT, it is necessary to understand the existing architecture and vulnerabilities of IoT, and establish an evaluation indicator system firstly. A widely accepted principle is that management is important for security evaluation. The S&R value is determined by the current situations of threat information, assets, vulnerability, and management, but no evaluation model is covering all these aspects. Moreover, most of the existing information security evaluation models are static snapshot-based evaluations, lacking dynamic feedback, and quantitative indicators of effectiveness.

By investigating existing security criteria, we note that a unified security evaluation framework and the evaluation model are still missing. Motivated by this observation, we attempt to build a comprehensive evaluation model covering threat information, assets, vulnerability, and management for IoT, and then we establish several quantitative indicators with aim of quantifying the model validity.

1.2 Architecture and vulnerability in IoT

Based on the IoT techniques, information can be exchanged efficiently among items, among objects and people with the real environment [Sun, Liu, Li et al. (2010)]. The

typical IoT network is normally constituted by the service-oriented three-layer architecture [Li, Li and Zhao (2014)] or 4-5 layers architecture that further divides the application layer [Lin, Yu, Zhang et al. (2017)].

The IoT system not only has the same security problems as traditional sensor networks, mobile communication networks and the Internet, but also has the unique security issues brought by the open nature of IoT. The security issues in the IoT include the data privacy issues, identity authentication and access control configuration issues, heterogeneous data storage and management strategies, etc. Details are given as follows.

Data and privacy protection issues: In the IoT system, data integrity and confidentiality are guaranteed by data encryption [Jing, Athanasios, Wan et al. (2014)]. Moreover, due to the limited computing power and resources of IoT devices, lightweight encryption is employed commonly. Besides, IoT devices contain a large amount of user private information, including location and upload frequency etc. That information is very sensitive to leakage.

Identity authentication and access control configuration issues: Aiming at the limited resources of the IoT terminal nodes and the vulnerability to attacks, in order to protect the privacy data of participants, lightweight identity authentication and fine-grained access control strategies are needed. The true identity of the communication participants and attackers can be determined through identity authentication, so the attacker can be identified in time [Jing, Athanasios, Wan et al. (2014); Orlando, Jacob, Khoa et al. (2015)].

Security issues of heterogeneous network convergence: The composition of IoT itself is the fusion of multiple heterogeneous networks. When dealing with the compatibility problems among networks, security problems are likely to occur [Jing, Athanasios, Wan et al. (2014)], resulting in a larger attack surface.

Massive heterogeneous data processing technology: The data format of various sensors in the sensing layer is different, the number of sensing terminals is huge. As a result, the IoT system has to load massive data. The IoT, cloud services [Abdur and Raffaele (2014)] and other new technologies are tightly integrated driven by the compression and fusion of massive data. The scope of security issue spans a range of data security itself and the security of various new technologies.

Management strategy and standard construction issues: The IoT needs to provide users with continuous and effective services, but the IoT system is exposed to diverse and complex environments, resulting in more exposed attack surfaces and higher instability. At the same time, there is a lack of unified standard specification and clear policy management for IoT.

There are excessive vulnerabilities in the IoT system, resulting in the difficulty of overall security evaluation as a whole.

1.3 Related researches and our contributions

In this subsection, we review some of the related researches on the security evaluation of IoT as follows.

The architecture and security privacy risk challenges of IoT are discussed in Hossain et al. [Hossain, Fotouhi and Hasan (2015); Yang, Wu, Yin et al. (2017)]. Hossain et al.

[Hossain, Fotouhi and Hasan (2015)] explored the architecture of IoT and revealed the security challenges and problems faced by the IoT. Yang et al. [Yang, Wu, Yin et al. (2017)] analyzed the security problems of different layers of the IoT. Nevertheless, these works only consider the attacks from the technical aspect while the security requirements at the management aspect are not analyzed.

Some researches investigate asset risk and dynamic performance of the IoT in information security evaluation. Jason et al. [Jason, Petar, Sadie et al. (2018)] investigated the key issues in security evaluation of the IoT, and put forward some assumptions through a series of seminars and interviews. The IoT security evaluation method may miss out asset risks if it uses periodic evaluations, regardless of possible changes in the IoT system (such as shifting boundaries).

The importance of management risk is discussed in Jason et al. [Jason, Petar, Sadie et al. (2018); Daniel, Kazem and Jacob (2017)]. Daniel et al. [Daniel, Kazem and Jacob (2017)] proposed a fine-grained Open Systems IoT Reference Model (OSiRM) model to analyze the security of the IoT and focused on three security-related mechanisms that include 1) authorization and authentication, 2) encryption and key management, 3) trust and identity management. This work indicates that during the IoT security evaluation, not only the risks faced by assets but also environmental risks and management risks should be considered. A comprehensive and dynamic evaluation framework in conjunction with the security evaluation methods should be sought for information security level analysis and evaluation.

The evaluation indicator system is discussed in works Lin et al. [Lin, Yu, Zhang et al. (2017)]. Lin et al. [Lin, Yu, Zhang et al. (2017)] pointed out that the security features of IoT including confidentiality, integrity, availability, authentication, privacy, and credibility. The security challenges and possible attacks of the perception layer, network layer and application layer are described in detail, which guides refining the secondary security indicators. Mario et al. [Mario, Pasquale, Gianluca et al. (2018)] pointed out that security and privacy issues are major challenges in IoT. At the same time, the security risks of IoT systems have been exacerbated due to inherent loopholes in terminal devices, limited resources, heterogeneous technologies, and the non-unified standards of the IoT system. The difference between IoT security issues and traditional computer security issues was summarized by Mario et al. [Mario, Pasquale, Gianluca et al. (2018)], including encryption algorithm magnitude, privacy data protection and large attack surfaces caused by open environments. This mentioned uniqueness indicates security target and performance metrics for the IoT.

The Evaluation model and method for information security evaluation in IoT are discussed in works [Mohammad (2016); Faisal, Abdullah and Sajjan (2018); Huang and Sun (2018)]. Mohammad [Mohammad (2016)] established a set of criteria to analyze the most suitable security frameworks for IoT. Its analysis follows the CC standard and gives an evaluation report. The shortcoming is that no specific evaluation algorithms are given. This work provides ideas for constructing an information security measurement system model and emphasizing the importance of management. Faisal et al. [Faisal, Abdullah and Sajjan (2018)] proposed a quantitative evaluation and comparison framework for the security and privacy evaluation of IoT using the analytic hierarchy process (AHP) method. Huang et al. [Huang and Sun (2018)] proposed an AHP-based risk evaluation

model to conduct a security risk evaluation for the core operating cloud platform of industrial IoT devices, enabling the Industrial IoT cloud platform to perform a self-examination. However, the evaluation indicators system of Huang et al. [Huang and Sun (2018)] lacks management risk.

Table 1: Related works on information security evaluation in IoT

Year	Author	Architecture of IoT	Security privacy risk and challenges faced	Asset risk	Manage ment risk	Evaluation model	Evaluation indicator system	Evaluation method
2018	[Mario, Pasquale, Gianluca et al. (2018)]	√	√	×	×	×	√	√
2017	[Lin, Yu, Zhang et al. (2017)]	√	√	×	×	×	√	×
2015	[Hossain, Fotouhi and Hasan (2015)]	√	√	×	×	×	×	×
2017	[Yang, Wu, Yin et al. (2017)]	√	√	×	×	×	×	×
2018	[Jason, Petar, Sadie et al. (2018)]	×	√	√	√	√	×	×
2017	[Daniel, Kazem and Jacob (2017)]	√	×	×	√	√	√	×
2016	[Mohammad (2016)]	√	×	×	×	√	×	×
2018	[Faisal, Abdullah and Sajjan (2018)]	×	×	×	×	√	√	√
2018	[Huang and Sun (2018)]	×	×	×	×	√	√	√

Tab. 1 summarizes the main focuses in related researches. Although most of the works focused on architecture, security privacy risk and challenges faced in IoT, and emphasized on building the evaluation indicator system and model. However, comparatively little work is done on formulating an overall evaluation indicator system containing asset risk and management risk, and giving specific evaluation algorithms. This paper proposed a comprehensive information security evaluation model based on multi-level decomposition feedback for quantifying S&R value in IoT that is built upon analyzing and complementing the previous works. The main contributions of this paper are summarized as follows.

1) We propose a comprehensive IoT information security evaluation model based on multi-level decomposition feedback to measure the security level and risk for IoT. This model consists of four main parts: building an evaluation indicator tree, calculating S&R through quantitative evaluation algorithms, guiding feedback strategy construction, and evaluating the validity of the model.

2) The proposed evaluation indicators comprehensively cover threat information, assets, vulnerability, and management to evaluate S&R value. To enhance the objectivity of the results, we build a core method with the confirmation algorithm based on the relationship between indicators and IM-TOPSIS algorithm to get final S&R value. The evaluation

model fixes the coverage problem of evaluation indicators and improves the objectivity of the quantitative evaluation.

3) We consider the relationship between residual risk and security investment to guild the establishment of a security reinforcement strategy. Moreover, we propose the residual risk, continuous risk conformity, head-to-tail consistency and decrease ratio to measure the model's validity. These indicators address issues that the validity of evaluation models cannot be measured.

The rest of this paper is organized as follows. Section II introduces the proposed multi-level decomposition feedback comprehensive IoT information security evaluation model. Section III explains the entire process of the evaluation model and verifies the validity of the algorithm using an example. Section IV concludes and discusses the possible future research directions.

2 Proposed model

Aiming at the problem of lack of a unified evaluation model in IoT systems, this paper divides the security analysis of IoT systems into two parts: external threat information and internal system information. Internal system information abstracts the traditional IoT layered architecture into three perspectives: asset, vulnerability, and management. According to the evaluation process of the existing CC standard, the comprehensive information security evaluation model based on multi-level decomposition feedback is proposed for the evaluation object in Fig. 1.

The information security evaluation model illustrates the evaluation framework and key considerations of IoT systems. The "dynamic" nature of the IoT has led to the need for continuous monitoring and evaluation of information security evaluations. A quantitative evaluation model will make it easier to provide information security risk level monitoring for IoT systems.

Firstly, we calculate the system protection rate and attack detection comprehensive index $F_{measure}$ [Thorsten (2005)] through analyzing the running scenarios, external threats and protective measures. Secondly, the input conditions for formalizing security targets are formed by analyzing the internal information of the system, including the requirements of assets, vulnerability, and management. Then, we analyze the corresponding set of security functions and build a metric model indicator tree system. Moreover, according to the metric algorithm library, select an appropriate algorithm to calculate comprehensive security results. Finally, we calculate the comprehensive output of the evaluation model to guide security decision makers to construct the security reinforcement strategy, which is used as feedback to enhance the security of the IoT system. The above process forms a closed loop to enhance the security of the IoT system.

The overall security level of the final output is set to five levels according to the requirements of the national level evaluation criteria: {high, higher, medium, lower, low}.

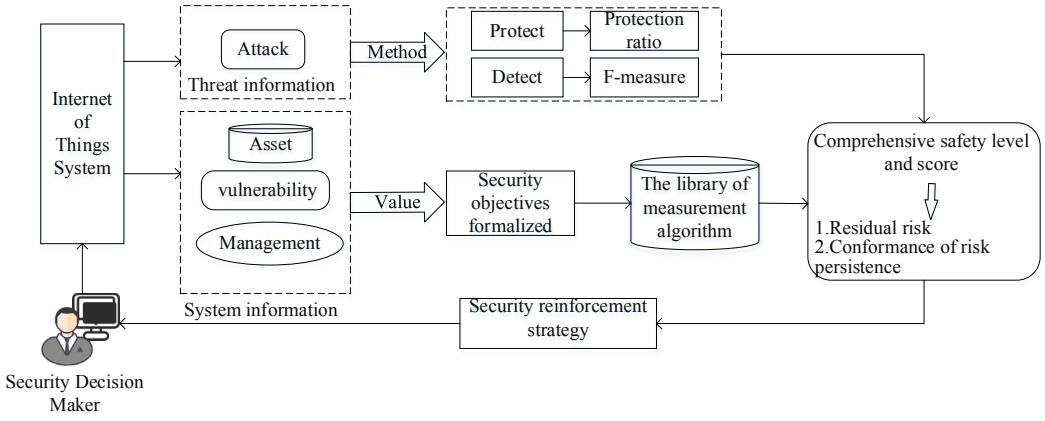

Figure 1: A comprehensive information security evaluation model based on multi-level decomposition feedback

2.1 Information security evaluation process

Under the guidance of the above comprehensive information security evaluation model, the specific process of information security evaluation for the IoT system is made. The evaluation process is divided into three parts as shown in Fig. 2.

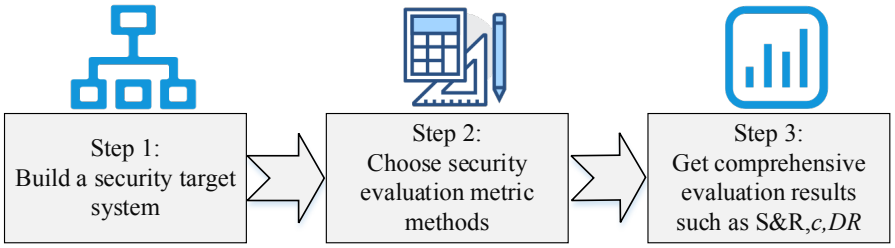

Figure 2: The evaluation process of the security evaluation model

Firstly, the strategic decomposition of the security objectives is proceeded by analyzing the characteristics of the evaluation object and then form the security target system. Secondly, the corresponding information security evaluation metric methods are chosen for calculating S&R quantitatively. Finally, on one hand, we use the risk continuous compliance (c) and residual risk (rr) to guide security decision makers to construct the security reinforcement strategy, which is used as feedback to enhance the security of the IoT system. On the other hand, we use the head-to-tail consistency (κ) and reduction ratio (DR) to judge the validity of the evaluation model.

2.2 Building a security target system

The establishment of a security target system is very important for the information security evaluation process of IoT systems. Given the unclear security targets of the IoT system, this paper formalizes the security targets into four primary indicators and eleven

secondary indicators according to the guidance of the evaluation criteria in Fig. 3. The four primary indicators are threat information, asset, vulnerability, and management. The eleven secondary indicators include system protection rate, attack detection rate, confidentiality, availability, controllability, identifiability, number of vulnerabilities, vulnerability hazard level, staff organization, enterprise grading, and service continuity.

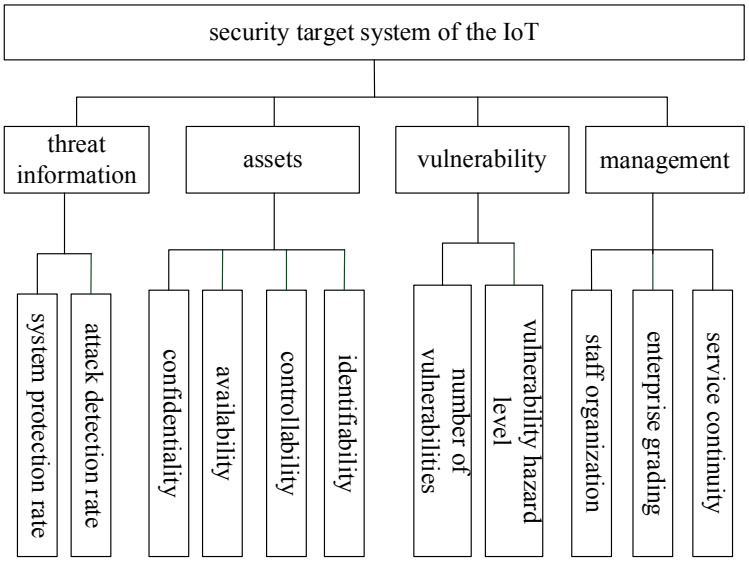

Figure 3: The security target system of the IoT system

2.3 Metric method

2.3.1 Calculation of attack protection rate and attack detection rate

Attack protection rate K refers to the degree of protection that can be achieved by analyzing the existing protection measures of the IoT system. It is calculated based on the ratio of the number of security measures that have been taken to the total number of sets of protection measures currently known to be used. we obtain the following equation:

$$K = \frac{\varpi \times a}{\Omega} \tag{1}$$

where ϖ indicates the weight of protective measures, a indicates the protective measures that have been taken and Ω represents a set of protection measures that are currently known to be made.

The attack detection rate comprehensive indicator $F_{measure}$ refers to the comprehensive evaluation of attack detection. For the protection measures in the IoT system, the attack detection system is an important part of the IoT security protection measures and it needs to be taken into account in calculating the security score of the overall IoT system.

We consider attack detection in the IoT system as a two-classifier and divide the judgment results into four types, as shown in Tab. 2.

Table 2: Judgment result of attack detection

System Input	System Judgment	
	Attack	Non-attack
Attack	TP	FN
Non-attack	FP	TN

The true positive (TP) indicates that the attack is correctly detected by the system and false negative (FN) indicates that the attack is not detected by the system. The false positive (FP) indicates that normal behavior is detected by the system as an attack and true negative (TN) indicates that the system correctly judges the normal behavior.

We obtain a composite score based on harmonic mean $F_{measure}$ to measure the quality of the results and the $F_{measure}$ is calculated as:

$$F_{measure} = \frac{2 \times TP}{2 \times TP + FN + FP} \tag{2}$$

2.3.2 Confirmation algorithm based on the relationship between indicators

The confirmation algorithm based on the relationship between indicators improved by the PageRank algorithm is based on the following assumptions: if the weight of other pointing links received by the node A is larger, then the node A is more important and the link node pointing to A has the better quality. The node with high quality will pass more weights to other nodes through the link, so the higher quality the node points to the node A, the more important node A is.

The formula for calculating the PR value of each node can be obtained as follows.

$$PR_{(p_i)} = \alpha \sum_{p_j \in M_{p_i}} \frac{PR_{(p_i)}}{L_{(p_j)}} + \frac{(1-\alpha)}{N} \tag{3}$$

where M_{p_i} is the set of nodes that are out of the chain, $L_{(p_j)}$ is the number of nodes p_j outbound, N is the total number of nodes and α is the probability that the user randomly arrives at a node, which is generally 0.85. The value of each node can be calculated by Eq. (3) and the final result can be obtained when the iteration tends to be stationary.

2.3.3 IM-TOPSIS security level determination algorithm

In this paper, we use the improved technique for order preference by similarity to an ideal solution (IM-TOPSIS) method to calculate the final safety score. TOPSIS is a sorting method that sorts of different objects based on how close they are to the idealized target [Supraja and Kousalya (2016); Wang, Lu and Gan (2017)]. The traditional TOPSIS method has two reference points: positive ideal solution and negative ideal solution. The scheme closes to the positive ideal solution and away from the negative ideal solution is the optimal solution. The IM-TOPSIS algorithm uses five levels of preset information security to evaluate the five-level ideal solution consisting of reference points and identifies the final result based on one of the five-level ideal solutions. This method can

be applied to evaluate our evaluation objects. Specific steps are as follows.

Step 1: Determine the original data matrix and the optimal solution matrix belonging to five levels.

According to the evaluation indicator system, the defined indicator set is {indicator 1, indicator 2, …, indicator n}, where n is the number of indicators. The comment set is defined as $C=\{c_1,c_2,\cdots,c_n\}=\{high,higher,medium,lower,low\}$.

The evaluation model uses the Delphi method to investigate the expert's evaluation of the fitness of each indicator at a safe level. The fitness evaluation rule is as follows. The evaluation value interval is [0, 1]. The higher the fitness, the closer the evaluation value is to 1 and the lower the fitness is, the closer the evaluation value is to zero.

With Delphi method, we can obtain the original evaluation matrix $P_{n\times5}$ is

$$P_{n\times5}=\begin{bmatrix} p_{11} & p_{12} & \cdots & p_{15} \\ p_{21} & p_{22} & \cdots & p_{25} \\ \vdots & \vdots & \ddots & \vdots \\ p_{n1} & p_{n2} & \cdots & p_{n5} \end{bmatrix}_{n\times5} \tag{4}$$

The optimal matrix is defined as a matrix belonging to a high security level, that is, the evaluation matrix is formed when each index reaches an optimal level. It is expressed as

$$P^1_{n\times5}=\begin{bmatrix} p_{11} & p_{12} & \cdots & p_{15} \\ p_{21} & p_{22} & \cdots & p_{25} \\ \vdots & \vdots & \ddots & \vdots \\ p_{n1} & p_{n2} & \cdots & p_{n5} \end{bmatrix}_{n\times5} \tag{5}$$

Similarly, the suboptimal matrix is defined as a matrix that belongs to a higher level, that is, the evaluation matrix is formed when each indicator reaches a suboptimal level. It is expressed as

$$P^2_{n\times5}=\begin{bmatrix} p_{11} & p_{12} & \cdots & p_{15} \\ p_{21} & p_{22} & \cdots & p_{25} \\ \vdots & \vdots & \ddots & \vdots \\ p_{n1} & p_{n2} & \cdots & p_{n5} \end{bmatrix}_{n\times5} \tag{6}$$

By analogy, the worst case matrix is defined as a matrix belonging to a low level, that is, the evaluation matrix is formed when each indicator reaches the worst level It is expressed as

$$P^5_{n\times5}=\begin{bmatrix} p_{11} & p_{12} & \cdots & p_{15} \\ p_{21} & p_{22} & \cdots & p_{25} \\ \vdots & \vdots & \ddots & \vdots \\ p_{n1} & p_{n2} & \cdots & p_{n5} \end{bmatrix}_{n\times5} \tag{7}$$

Step 2: Calculate the evaluation scores of each indicator and the optimal solution of five grades.

We create a rating level weight set $U=[u_1,u_2,u_3,u_4,u_5]$. The set of indicator weights calculated by the weighting algorithm based on the relationship between the indicators is

$W = [w_1, w_2, \cdots, w_n]$.

Let $W^{'} = Diag(w_1, w_2, \cdots, w_n)$ and the evaluation score set for each indicator is calculated as $S = W^{'} \times P \times U^T = \left[s_1, s_2, \cdots, s_n \right]^T$.

Therefore, the high-level ideal solution is $S^1 = W^{'} \times P^1 \times U^T = \left[s_1^1, s_2^1, \cdots, s_n^1 \right]^T$.

Similarly, the higher-level ideal solution is $S^2 = W^{'} \times P^2 \times U^T = \left[s_1^2, s_2^2, \cdots, s_n^2 \right]^T$.

By analogy, the low-level ideal solution is $S^5 = W^{'} \times P^5 \times U^T = \left[s_1^5, s_2^5, \cdots, s_n^5 \right]^T$.

Step 3: Calculate the Euclidean distance of the evaluation object to the five-level optimal solution.

We calculate the Euclidean distance of the evaluation object to the five-level optimal solution according to the equation $d^j = \sqrt{\sum_{i=1}^{n} (s_i - s_i^j)^2} \quad (j = 1, \cdots, 5)$.

Step 4: Normalize the five Euclidean distances to build a weight matrix.

Firstly, through the calculation in Step 3, we get the vector Z as follows.

$$Z = [1 - \frac{d^1}{\sum_{i=1}^{5} d^i}, 1 - \frac{d^2}{\sum_{i=1}^{5} d^i}, \cdots, 1 - \frac{d^5}{\sum_{i=1}^{5} d^i}] \tag{8}$$

Finally, we use the softmax function to obtain the normalized weight vector and get $B = [b_1, b_2, \cdots, b_5]$, where

$$b_j = \frac{e^{z^j}}{\sum_{k=1}^{5} e^{z^k}} \tag{9}$$

2.3.4 Indicator of measurement

1) Safety core and risk value

The interval for setting the security level and score is shown in Tab. 3.

Table 3: Judgment result of attack detection

Security Level	Low	Lower	Medium	Higher	High
Score Interval	[0, 0.2]	(0.2, 0.4]	(0.4, 0.6]	(0.6, 0.8]	(0.8, 1]

The vector formed by the upper limit of the interval is $M = [m_1^{\max}, m_2^{\max}, \cdots, m_5^{\max}]$. Therefore, the safety score (s) is calculated as follows.

$$s = \lambda_1 \cdot B \times M^{'} + \lambda_2 \cdot K \cdot F_{measure} \tag{10}$$

where λ_1 and λ_2 represent the weight ratio of external threat information and internal system information, which are generally set to 0.5. K is the attack protection rate and $F_{measure}$ is the attack detection rate.

The risk score (r) is calculated as $r = 1 - s$, where s refers to the calculated comprehensive safety score.

2) Residual risk and security investment

Residual risk (rr) is the residual value of the IoT system after adding security investment and adopting a security reinforcement strategy, that is, the result of secondary security evaluation.

Security investment (v) refers to additional security cost that result in the risk value within a defined acceptable range. As security investment increases, the residual risk gradually declines. In system services, it is suitable to use game theory to analyze the relationship between system security residual risk and security investment. In this paper, the discussion of the ideal state does not consider the commercial benefits of security investment, only the reduced risk.

For the evaluation and control of security risks, it is not the pursuit of risk values as small as possible. Because it takes a price to reduce the risk, whether it is to take measures to reduce the possibility of a security incident, or to reduce the possible losses caused by security incidents, systems need a corresponding security investment. The correct approach is to limit the security risk to an acceptable level to maintain basic functions. According to the risk factors, we can optimize the safety limit of each first-level safety target, seek the best security investment plan, and get a high level of safety value.

Generally, as security investment increases, security residual risk decreases. The researches on the optimal information system security investment can be traced back to the Gordon-Rob model of the early 21st century. Work by Gordon et al. [Gordon and Loeb (2002)] considers the relationship between security investment and security breach. In this paper, we refer to this idea and consider the relationship between security investment and security residual risk vulnerability. The rr vulnerability depending on the security investment v and the risk vulnerability of the system r ($r \in [0,1]$) and it is calculated as follows.

$$rr = f_v(r, v) = r^{\psi v + 1} \tag{11}$$

where the parameter $\psi > 0$ is the intensity of security investment on security risk.

Take a data simulation to describe the relationship between security residual risk and security investment as shown in Fig. 4. We set $\psi = 0.3$. Three kinds of original risk vulnerability are shown by $rr = 0.3, 0.6, 0.9$ in the figure. The figure shows that with an increase in security investment, three curves of security residual risk decrease from the original rr value to almost zero.

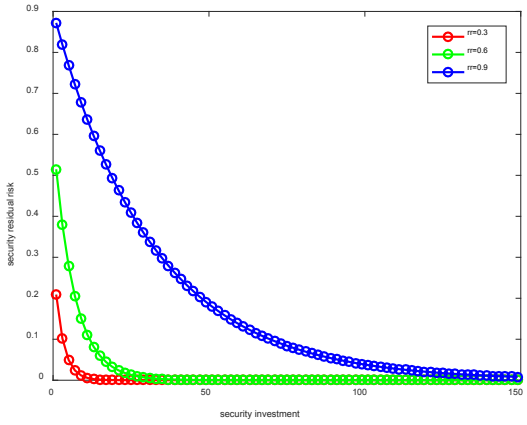

Figure 4: The relationship between security residual risk and security investment

3) Continuous conformity of residual risk

The comprehensive information security evaluation model based on multi-level decomposition feedback can judge the security stability of the evaluation object according to the continuous conformity (c) of residual risk in the evaluation process. The c of residual risk refers to the absolute difference between the residual risk value and the ideal risk value obtained after a series of security evaluations. The information security evaluation is measured in units of days. After multiple security evaluations, the c of residual risk of the evaluation object is calculated as follows.

$$c = | X - \overline{X} | \tag{12}$$

where X and $\overline{X}$ denote to the residual risk value obtained for each security evaluation and the ideal value of the residual risk which is generally set to zero, respectively. The result interval of c is [0,1] and the closer the result is to 0, the better c is. By plotting the curve function of the c of residual risk, the trend of the degree of closeness between the evaluated system and the ideal state can be obtained.

4) Head-to-tail consistency and decrease ratio

In order to better judge the validity of the evaluation model, two indicators of head-to-tail consistency and decrease ratio are proposed. Suppose there are evaluation objects, and we use different evaluation methods to get the results ranking. Then, we find the number x of common objects in the best 40% of the objects and the number y of common objects in the worst 40% objects by doing the descending order. The formula for calculating the head-to-tail consistency rate (κ) is as follows.

$$\kappa = \frac{x + y}{0.8 \times m} \tag{13}$$

Obviously, the closer the result of the above formula is to 1, the better.

For decrease ratio (DR), if there are m evaluation objects and the descending order is

arranged according to the level of the score f. Then, the function $f(N)$ of f concerning the sorted object number N is a monotonically decreasing function. The coordinate of the best object for the evaluation result is $(1, f(1))$ and the worst object for the evaluation result is $(m, f(m))$. The formula for calculating DR is as follows.

$$DR = \frac{\sum_{i=1}^{m} \sqrt{(V_{i+1} - V_i)^2 + (N_{i+1} - N_i)^2}}{\sqrt{(V_m - V_1)^2 + (N_m - N_1)^2}} \tag{14}$$

In order to remove the influence of different scale values, the evaluation scores are standardized. Let $[0, m]$ is the processed score interval set, where $(1, m)$ and $(m, 0)$ represent the maximum point coordinate and the minimum point coordinate, respectively. The standardization formula is as follows.

$$V_i = m \times (1 - \frac{|V_i^{'} - V_1^{'}|}{V_1^{'} - V_m^{'}}) \tag{15}$$

where $V_i^{'}$ is the evaluation result before standardization and V_i is the evaluation result after standardization. Therefore, the standardized DR is as follows.

$$DR = \frac{\sum_{i=1}^{m} \sqrt{(V_{i+1} - V_i)^2 + 1}}{\sqrt{2m^2 - 2m - 1}} \tag{16}$$

The DR refers to the ratio of the sum of adjacent two points' Euclidean distances in the evaluation result to the distance between the first and last points. The comparison between a high decrease ratio and a low decrease ratio is shown in Fig. 5. If the value is lager, the scatter distribution is in the shape of a star line in the figure. This will result in partial interval points being concentrated and some interval points being scattered. Moreover, the evaluation is blurred within the concentrated range of values. If the value is closer to 1, it means that all the data show a uniform downward trend and better model performance.

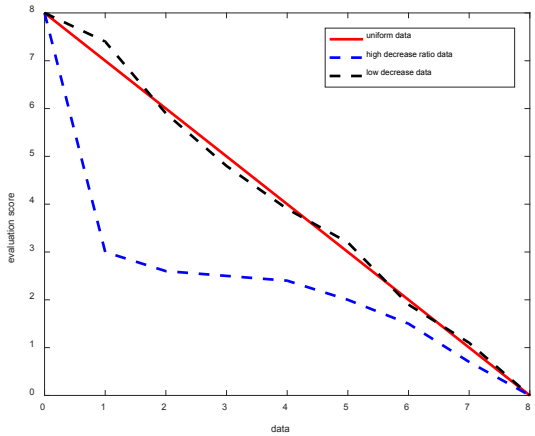

Figure 5: Data distribution with different decreasing ratios

3 Data and evaluation results

We evaluate the comprehensive information security evaluation model based on multi-level decomposition feedback through an example of the IoT system and get evaluation results.

3.1 Evaluation target

We first divide the security target indicators of the evaluation object and analyze the vulnerability of each indicator. The first-level indicators of the information security target system of the evaluation object are identified as four categories: threat information, assets, vulnerability, and management. The secondary indicators are determined as eleven categories: system protection rate, attack detection rate, confidentiality, availability, controllability, identifiability, number of vulnerabilities, vulnerability hazard level, staff organization, enterprise grading and service continuity.

3.2 Evaluation results

3.2.1 Attack protection rate and attack detection rate

The collection of protection data and attack data is performed for the evaluation object. Through the Delphi method and objective data, the actual protective measures data are shown in Tab. 4. According to the contents of Tab. 4, the attack protection rate $K = 0.6$ is calculated.

Table 4: The list for investigation of protective measures

Protective Measures	Weights	Protection Situation
Firewall	0.3	reached the standard
Attack detection system	0.3	reached the standard
Flow monitoring	0.2	failed to meet the standard
Artificial patrol	0.2	failed to meet the standard

We conducted 1000 simulated attack tests on the attack detection system and the judgment results are shown in Tab. 5.

Table 5: The attack detection judgment result

System Input	System Judgment	
	Attack	Non-attack
Attack	750	88
Non-attack	62	100

According to Eq. (2), we can calculate $F_{measure}$=0.91 .

3.2.2 Weights calculation

In this paper, the weights of nine secondary indicators in the evaluation object are determined through the confirmation algorithm based on the relationship between

indicators. The nine secondary indicators including confidentiality, availability, controllability, identifiability, number of vulnerabilities, vulnerability hazard level, staff organization, enterprise grading and service continuity. According to 20 experts' scores, we build an expert score sheet as shown in Tab. 6. The adjacency matrix Q is constructed according to the expert evaluation results obtained by the Delphi method. Then, the column vector in the adjacency matrix Q is normalized to obtain the probability transition matrix H, where the i th row and j th column in the expert score table represent the number of people who believe that the i th indicator will affect the j th indicator.

Table 6: The expert score table of indicator relationship

	U_1	U_2	U_3	U_4	U_5	U_6	U_7	U_8	U_9
U_1	0	15	16	16	5	3	5	2	16
U_2	12	0	13	15	3	4	3	2	15
U_3	15	11	0	14	5	4	3	2	15
U_4	13	10	17	0	3	3	2	5	15
U_5	17	18	17	17	0	3	3	2	5
U_6	15	16	16	17	5	0	2	2	17
U_7	14	15	15	14	8	3	0	5	18
U_8	13	12	15	14	4	3	17	0	16
U_9	15	17	12	11	5	4	3	3	0

The constructed adjacency matrix Q and probability transfer matrix H are

$$Q=\begin{bmatrix} 0 & 15 & \cdots & 16 \\ 12 & 0 & \cdots & 15 \\ \vdots & \vdots & \ddots & \vdots \\ 15 & 17 & \cdots & 0 \end{bmatrix}_{9\times 9} \text{ and } H=\begin{bmatrix} 0 & 0.3655 & \cdots & 0.3681 \\ 0.2961 & 0 & \cdots & 0.3451 \\ \vdots & \vdots & \ddots & \vdots \\ 0.3702 & 0.4143 & \cdots & 0 \end{bmatrix}_{9\times 9}.$$

The final transfer matrix G is calculated by the follows.

$$G=\alpha\cdot S+\frac{1-\alpha}{N}\cdot U \tag{17}$$

where U is an $n\times n$ matrix of all ones and N is the number of indicator nodes.

We use the final transfer matrix G to calculate the weight vector P_n after repeated iterations. The calculation formula is as follows.

$$P_{n+1}=G\cdot P_n \tag{18}$$

where the value of P_n is a column vector composed of probability values after the n th

iteration.

The final P_n value constitutes the weight vector W of each secondary indicator and $W = [0.151,\ 0.146,\ 0.158,\ 0.150,\ 0.064,\ 0.053,\ 0.071,\ 0.049,\ 0.158]$.

3.2.2 Calculation of the comprehensive evaluation result

In this paper, the IM-TOPSIS security level determination algorithm is used to calculate the security level and security score for the nine indicators. The expert scoring table is constructed as shown in Tab. 7 and the evaluation matrix $P_{9\times5}$ is obtained based on the expert scoring results.

Table 7: The experts' score of evaluation index

Evaluation Indicator	High	Higher	Medium	Lower	Low
U_1	5	34	27	26	8
U_2	8	23	24	30	15
U_3	20	23	17	20	20
U_4	13	33	18	15	21
U_5	5	47	33	7	8
U_6	18	38	26	10	8
U_7	0	60	23	10	8
U_8	4	45	34	14	3
U_9	0	0	65	32	3

Therefore, the evaluation matrix is $P = \begin{bmatrix} 0.05 & 0.34 & \cdots & 0.08 \\ 0.08 & 0.23 & \cdots & 0.15 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0.03 \end{bmatrix}_{9\times9}$.

The subjective weight of different safety levels determined by the Delphi method is $U = [\frac{1}{15}, \frac{2}{15}, \frac{1}{5}, \frac{4}{15}, \frac{1}{15}]$. Then we calculate the Euclidean distance of the evaluation object's result from the five-level ideal solution. The Euclidean distance is normalized to obtain the membership vector $B = [0.1738, 0.2014, 0.2034, 0.2175, 0.1738]$. In the end, the safety score is $s = 0.5746$.

3.2.4 Measure indicators

Based on the above calculations, we get the risk score is $r = 1 - s = 0.4254$. So, there is a medium risk in the evaluation object.

From Eq. (11), we can get the relationship between investment and residual risk is

$$v = \frac{\frac{\log rr}{\log r} - 1}{\psi} \tag{19}$$

If we are pursuing a system ideal state with $rr = 0.1$, then we can judge our security investment status according to Eq. (19) is $v = 5.646$.

In two natural months, the security evaluation of the evaluation object was repeated every 7 days for a total of 9 times by different methods. One way is the IM-TOPSIS security level determination algorithm we proposed and the other way is the fuzzy comprehensive evaluation algorithm. The results of the information security evaluation are shown in Fig. 6. By analyzing the results in the figure, we can get the IM-TOPSIS method performs better in quantifying S&R of evaluation object.

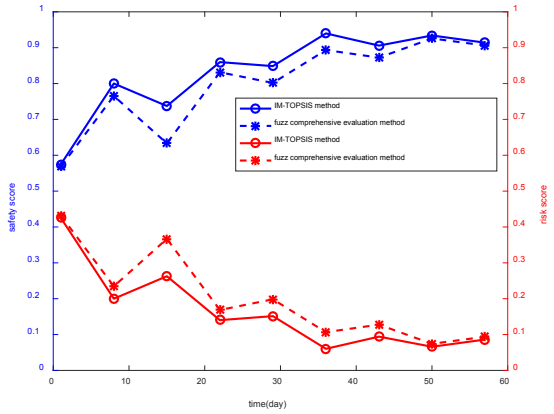

Figure 6: Comparison of safety scores and risk values calculated by different methods

The calculated residual risk continuous conformity is shown in Fig. 7. As the system continues to be monitored, it continues to be stable and tends to be close to the ideal state.

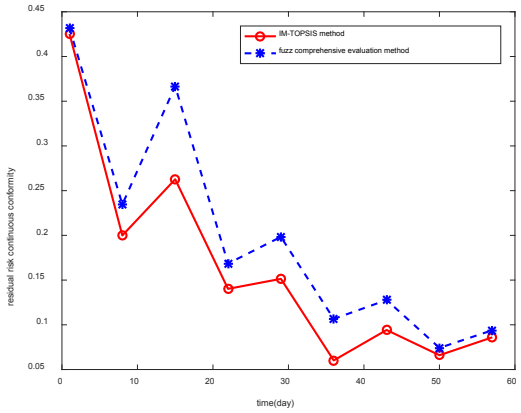

Figure 7: The continuous conformity calculated by the IM-TOPSIS method

In order to better verify the validity of the model in this paper, we choose the subjective weighting method for comprehensive comparison in addition to the above two methods. The subjective weighting method is also known as the Delphi method. We choose five different IoT systems as evaluation objects and we get the safety score and ranking as shown in Tab. 8. We calculate the head-to-tail consistency κ and the decrease ratio DR through Eqs. (13)-(17). It is calculated that the κ of the three methods are the same, but the model proposed in this paper has a relatively low decrease ratio with 1.1085. Therefore, the model proposed in this paper has better validity.

Table 8: The result of safety score and ranking

Object Number	The subjective weighting method		Fuzzy comprehensive evaluation		**IM-TOPSIS method**	
	Ranking	Safety score	Ranking	Safety score	Ranking	Safety score
1	4	0.7963	5	0.6540	4	0.7105
2	1	0.9245	1	0.7853	1	0.9023
3	3	0.8024	3	0.6874	3	0.7965
4	5	0.7853	4	0.6652	5	0.7045
5	2	0.8179	2	0.6983	2	0.8157
DR	1.1531		1.1113		**1.1085**	
κ	0.75		075		**0.75**	

4 Conclusion

Security challenges faced by the IoT are obstacles to IoT success. To solve the problem that there is a lack of unified security framework and model, this paper proposes a comprehensive information security evaluation model based on multi-level decomposition feedback to quantify the S&R status of the IoT system. The evaluation model includes three important parts, (1) a security target system which includes four primary indicators and eleven secondary indicators, (2) the core evaluation algorithm part where we choose the weighting algorithm based on the relationship among indicators and the IM-TOPSIS quantifying method, (3) the evaluation indicators we proposed to supervise the validity, such as residual risk, head-to-tail consistency and decrease ratio. Also, this work provides help to standards organizations in better understanding the security features of IoT and designing a unified security evaluation framework and model.

In the future, we will expand the core algorithm library and build an adaptation evaluation model based on the characteristics of security evaluation indicators and national security evaluation criteria.

Acknowledgement: The authors would like to thank anonymous reviewers who read drafts and made many helpful suggestions.

Funding Statement: This work was supported in part by National Key R&D Program of China under Grant 2019YFB2102400 and in part by the BUPT Excellent Ph.D. Students Foundation under Grant CX2019117.

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

References

Abdur, R. B.; Raffaele, G. (2014): IoT and cloud convergence: Opportunities and challenges. *IEEE World Forum on Internet of Things*, pp. 375-376.

CCRA. (2019): Common criteria for information technology security evaluation. https://www.commoncriteriaportal.org/cc/.

Daniel, M.; Kazem, S.; Jacob, K. (2017): IoT security (IoTSec) considerations, requirements, and architectures. *14th IEEE Annual Consumer Communications Networking Conference*, pp. 1006-1007.

Emanuele, C.; Diego, C.; Gerd, K.; Stefano, M.; Andrea, P. et al. (2017): Probabilistic risk-based security assessment of power systems considering incumbent threats and uncertainties. *IEEE Power Energy Society General Meeting*, pp. 1.

Faisal, A.; Abdullah, A.; Sajjan, S. (2018): Quantifying security and privacy in Internet of Things solutions. *IEEE/IFIP Network Operations and Management Symposium*, pp. 1-6.

Gordon, L. A.; Loeb, M. P. (2002): The economics of information security investment. *ACM Transactions on Information and System Security*, vol. 5, no. 4, pp. 438-457.

He, S. M.; Xie, K.; Xie, K. X.; Xu, C.; Wang, J. (2019): Interference-aware multisource transmission in multiradio and multichannel wireless network. *IEEE Systems Journal*, vol. 13, no. 3, pp. 2507-2518.

Hossain, M. M.; Fotouhi, M.; Hasan, R. (2015): Towards an analysis of security issues, challenges, and open problems in the Internet of Things. *IEEE World Congress on Services*, pp. 21-28.

Huang, Y.; Debnath, J.; Iorga, M.; Kumar, A.; Xie, B. (2019): CSAT: a user-interactive cyber security architecture tool based on NIST-compliance security controls for risk management. *IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference*, pp. 697-707.

Huang, Y.; Sun, W. (2018): An AHP-based risk assessment for an industrial IoT cloud. *IEEE International Conference on Software Quality, Reliability and Security Companion*, pp. 637-638.

Hui, H.; Zhou, S.; Xu, S.; Lin, F. (2020): A novel secure data transmission scheme in industrial internet of things. *China Communications*, vol. 17, no. 1, pp. 73-88.

Jason, R. C.; Petar, R.; Sadie, C.; David, D. (2018): If you can't understand it, you can't properly assess it! the reality of assessing security risks in Internet of Things systems. *IET Living in the Internet of Things: Cybersecurity of the IoT Conference*, pp. 1-9.

Jing, Q.; Athanasios, V.; Wan, J.; Lu, J.; Qiu, D. (2014): Security of the Internet of Things: perspectives and challenges. *Wireless Networks*, vol. 20, no. 8, pp. 2481-2501.

Li, L.; Li, S.; Zhao, S. (2014): Qos-aware scheduling of services-oriented Internet of Things. *IEEE Transactions on Industrial Informatics*, vol. 10, no. 2, pp. 1497-1505.

Li, S.; Bi, F.; Chen, W.; Miao, X.; Liu, J. et al. (2018): An improved information

security risk assessments method for cyber-physical-social computing and networking. *IEEE Access*, vol. 6, pp. 10311-10319.

Lin, F.; Zhou, Y.; An, X.; You, I.; Choo, K. (2018): Fair resource allocation in an intrusion-detection system for edge computing: ensuring the security of Internet of Things devices. *IEEE Consumer Electronics Magazine*, vol. 7, no. 6, pp. 45-50.

Lin, F.; Zhou, Y.; You, I.; Lin, J.; An, X. et al. (2019): Content recommendation algorithm for intelligent navigator in fog computing based IoT environment. *IEEE Access*, vol. 7, pp. 53677-53686.

Lin, J.; Yu, W.; Zhang, N.; Yang, X.; Zhang, H. et al. (2017): A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125-1142.

Mario, M.; Pasquale, P.; Gianluca, A.; Giancarlo, F. (2018): Evaluating critical security issues of the IoT world: Present and future challenges. *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2483-2495.

Medhane, D. V.; Sangaiah, A. K.; Hossain, M. S.; Muhammad, G.; Wang, J. (2020): Blockchain-enabled distributed security framework for next generation IoT: an edge-cloud and software defined network integrated approach. *IEEE Internet of Things Journal*, https://doi.org/10.1109/JIOT.2020.2977196.

Mohammad, I. (2016): A systematic review of information security frameworks in the Internet of Things (IoT). *IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems*, pp. 1270-1275.

Orlando, A.; Jacob, W.; Khoa, H.; Jin, Y. (2015): Privacy and security in Internet of Things and wearable devices. *IEEE Transactions on Multi-Scale Computing Systems*, vol. 1, no. 2, pp. 99-109.

P. N. Technology. (2018): The latest survey shows that computers, mobile phones and other devices suffer an attempted cyber attack every five minutes (1st ed). http://tech.ifeng.com/c/7irmcLeXUsS.

Su, J.; Lin, F.; Zhou, X.; Lu, X. (2015): Steiner tree based optimal resource caching scheme in fog computing. *China Communications*, vol. 12, no. 8, pp. 161-168.

Sun, Q.; Liu, J.; Li, S.; Fan, C.; Sun, J. (2010): Internet of Things: summarize on concepts, architecture and key technology problem. *Journal of Beijing University of Posts and Telecommunications*, vol. 33, no. 3, pp. 1-9.

Sun, W.; Cai, Z.; Li, Y.; Liu, F.; Fang, G. et al. (2018): Security and privacy in the medical Internet of Things: a review. *Security and Communication Networks*, vol. 2018, pp. 1-9.

Supraja, S.; Kousalya, P. (2016): A comparative study by AHP and TOPSIS for the selection of all round excellence award. *International Conference on Electrical, Electronics, and Optimization Techniques*, pp. 314-319.

Thorsten, J. (2005): A support vector method for multivariate performance measures. *Proceedings of the 22Nd International Conference on Machine Learning*, pp. 377-384.

Wang, B.; Kong, W.; Guan, H.; Xiong, N. (2019): Air quality forecasting based on

gated recurrent long short term memory model in Internet of Things. *IEEE Access*, vol. 7, pp. 69524-69534.

Wang, B.; Kong, W.; Li, W.; Xiong, N. (2019): A dual-chaining watermark scheme for data integrity protection in Internet of Things. *Computers, Materials and Continua*, vol. 58, no. 3, pp. 679-695.

Wang, D.; Lu, Y.; Gan, J. (2017): An information security evaluation method based on entropy theory and improved TOPSIS. *IEEE Second International Conference on Data Science in Cyberspace*, pp. 595-600.

Yang, Y.; Wu, L.; Yin, G.; Li, L.; Zhao, H. (2017): A survey on security and privacy issues in Internet-of-Things. *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250-1258.

Zhou, W.; Jia, Y.; Peng, A.; Zhang, Y.; Liu, P. (2019): The effect of IoT new features on security and privacy: new threats, existing solutions, and challenges yet to be solved. *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1606-1616.