Computers, Materials & Continua
DOI:10.32604/cmc.2021.016623
Article

Tech Science Press

Security-Critical Components Recognition Algorithm for Complex Heterogeneous Information Systems

Jinxin Zuo[1,2], Yueming Lu[1,2,*], Hui Gao[2,3], Tong Peng[1,2], Ziyv Guo[2,3], Tong An[1,2] and Enjie Liu[4]

[1]School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing, 100876, China
[2]Key Laboratory of Trustworthy Distributed Computing and Service (BUPT), Ministry of Education, Beijing, 100876, China
[3]School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing, 100876, China
[4]University of Bedfordshire, Institute for Research in Applicable Computing (IRAC), Luton, UK
[*]Corresponding Author: Yueming Lu. Email: ymlu@bupt.edu.cn
Received: 06 January 2021; Accepted: 12 February 2021

Abstract: With the skyrocketing development of technologies, there are many issues in information security quantitative evaluation (ISQE) of complex heterogeneous information systems (CHISs). The development of CHIS calls for an ISQE model based on security-critical components to improve the efficiency of system security evaluation urgently. In this paper, we summarize the implication of critical components in different filed and propose a recognition algorithm of security-critical components based on threat attack tree to support the ISQE process. The evaluation model establishes a framework for ISQE of CHISs that are updated iteratively. Firstly, with the support of asset identification and topology data, we sort the security importance of each asset based on the threat attack tree and obtain the security-critical components (set) of the CHIS. Then, we build the evaluation indicator tree of the evaluation target and propose an ISQE algorithm based on the coefficient of variation to calculate the security quality value of the CHIS. Moreover, we present a novel indicator measurement uncertainty aiming to better supervise the performance of the proposed model. Simulation results show the advantages of the proposed algorithm in the evaluation of CHISs.

Keywords: Complex heterogeneous information system; security-critical component; threat attack tree; information security quantitative evaluation

1 Introduction

With the development of emerging technologies such as edge computing, big data, internet of things [1–7], information systems are evolving constantly. The heterogeneity of information systems is also increasing. To continuously supervise the security status of information systems and improve the security capabilities and compliance of information systems, it often needs to repeat the process of information security quantitative evaluation (ISQE) by a monitoring system, iteratively [8]. However, traditional ISQE targets have characteristics of strong independence and low coupling among the modules, so it can only be evaluated as a whole [9]. With the

establishment of information security certification and accreditation system, the scope of certification has gradually extended from IT products, network critical equipment, network security products to services, systems, etc. [10]. The currently included evaluation targets are divided into more detailed modules, which have poor applicability to CHISs.

Connecting humans and objects through public or private networks are gradually becoming the Cyber-Physical System (CPS) or the Internet of Things (IoT) Information System [11]. The IoT information system is a combination of wireless sensor networks (WSNs), computer networks, and cloud computing networks. As a representation of CHISs, the IoT information system has the characteristics of limited terminal resources, low power consumption, high availability, and high connectivity. The growth of the number of IoT information systems is a future trend. It is predicted that the number of IoT devices will reach 125 billion in 2030 [11]. The architecture of the IoT information systems is mainly divided into three levels: "cloud-edge-terminal," however, the specific topology structure may change over time. Therefore, it is necessary to construct the network topology through asset mapping to clarify the asset archives of the information system. With the large-scale deployment and application of the IoT information systems as well as frequent attacks, the security privacy protection and security evaluation of the IoT information system is still the direction of high attention [12–20]. The diversified application scenarios and complex topology of the IoT information system have brought challenges to its information security quantitative evaluation.

1.1 Motivation

To address the efficiency issues of ISQE in CHISs, numerous researchers devote themselves to the formalization of the evaluation target and risk evaluation of CHISs. The comprehensive information security quantitative security evaluation for CHISs is a theoretically expected solution.

However, due to the complex network topology and diverse data sources of CHISs, selecting security-critical components of CHISs can improve the efficiency and real-time nature of ISQE. To enhance the applicability of the ISQE model and improve the efficiency and effectiveness of the ISQE process, it is necessary to investigate and analyze the security architecture of the evaluated target, construct its description method, and abstract its security-critical components (set) to improve information the efficiency of security quality evaluation.

By investigating existing researches, we note that a recognition algorithm of security-critical components for evaluation targets is still missing. Motivated by this observation, we attempt to build a recognition algorithm of security-critical components for the CHIS, and then we establish a quantitative indicator with aim of quantifying the model validity.

1.2 Related Works

To evaluate the information security quality of CHISs more efficiently, it is necessary to deal with the prominent contradiction between the system status update and the security requirements increase. The security-critical components (set) are selected in the process of formalizing the security function of the evaluation object, and it can help realize the formalization of the target of evaluation (ToE). The formalization of the security function of the evaluation object is very important to the overall ISQE. In the ISQE of CHISs, the security-critical components (set) are defined as core components that have an important impact on the information system in terms of security and may cause security problems. Constructing the security-critical components (set) of the evaluation object is the basis for completing the formalization of the security target of the evaluation object.

Among the current information security standards, the Common Criteria (CC) provides a solution based on the (Protection Profile (PP) module [21]. It can use basic PP to describe the core security function requirements of a class of products and increase the deformation requirements and new requirements by compiling PP modules, and further improve the protection profile of the evaluation object. The specific construction process of the protection profile is shown in Fig. 1.

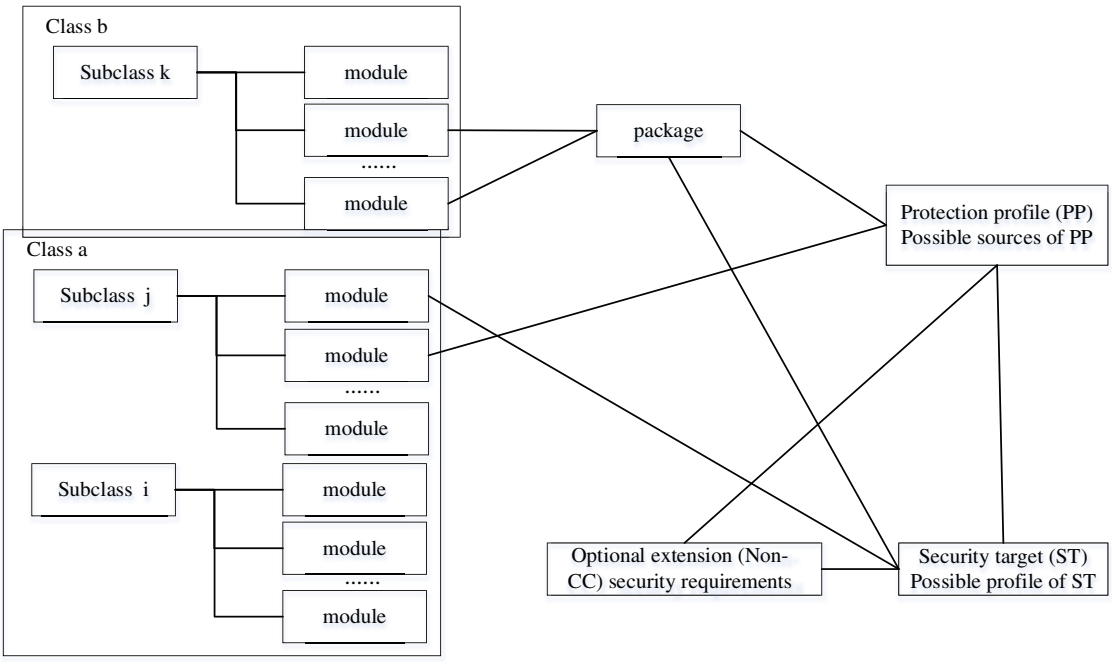

Figure 1: Specific construction process of the protection profile

The traditional definition of critical components is mostly carried out from the perspective of functionality and reliability analysis. From the perspective of production, critical components are generally defined as parts that have a long production cycle, complex processing, occupy a lot of resources, and require separate and safe production. From the perspective of functionality, critical components generally refer to the main functional components of the product [22]. From the perspective of information security, security-critical components are defined as core components that have an important impact on systems, products, and services in terms of security, and may cause security problems.

Many researchers have carried out selection and tracking studies of critical components in different fields. Xu [23] used RFID technology to track the key parts of the common rail pipe in the high-pressure common rail system, where the TOPSIS method was adopted to prioritize the replacement parts and then guided the production and management of the enterprise. According to the design parameters of the top drive system of a certain type of coalbed methane drilling rig, Lv [24] analyzed and designed the key components of the top drive system. Sun [25] studied the methods and procedures for identifying critical parts of reliability and quality in the identification of key parts of military-industrial enterprises and provided support for the model development process. To improve the overall safety level of military aircraft, Shi et al. [26] analyzed the management standards and *status quo* of the critical safety items of the US military aviation and

then suggested that domestic management requirements and standards for the critical safety items of our military should be established. For the identification of key software components, Sheng et al. [27] proposed an identification method based on the characteristic index fault forest model.

In the field of network security, there are some researches on the identification and tracking of critical components. In the process of information security certification and accreditation, Tao et al. [28] designed a threat tree-based identification algorithm for critical components of IT products in response to repeated evaluations and long evaluation cycles caused by IT product update iterations. The above algorithm provides a basis for product change control in information security certification.

In terms of network equipment identification and spatial asset mapping, most of the existing cyberspace mapping systems use active or passive detection methods to draw device portraits in cyberspace and construct network topologies. For example, it is known that ZoomEye of Chuangyu Company [29], Qi'anxin Global Hawk System [30], Shodan cyberspace equipment search engine [31], etc., can detect infrastructure in some parts of the world, such as routing equipment, industrial networking equipment, IoT equipment, etc. Using search engine technology, users can use various filters to find specific types of devices connected to the Internet. The AMIT and MR-Net projects carried out by the ANT laboratory detect the current use of Internet resources, track the changing trends of topology and traffic, and mark relevant information on the network map to help researchers better improve network security and increase defensive ability. However, most of the current spatial mapping systems focus on the assets and open ports exposed in the public network of cyberspace, and there are fewer products for identifying and mapping specific information system assets. But the methods can be applied to enhance the breadth of basic data for ISQE. Aiming at the problem of device identification in virtual network space, Li [32] studied the network device identification system and realized the classification and identification of the network device system through network scanning, traffic collection, and decision tree algorithm. Yang et al. [33] proposed a method for identifying IoT devices based on traffic fingerprints, using the forest classification algorithm to identify and judge the types of devices newly connected to the Internet of Things. It provides support for the further construction of threat perception models.

We can use asset mapping and threat modeling as the basis for the identification of security-critical components (sets). By introducing the above technologies into the field of ISQE, the breadth of basic data for ISQE has been expanded. Based on the tracking and identification of security-critical components, we have simplified the tedious index combing process in the iterative evaluation process of the system and focused on important security-critical components. The model proposed in this paper can improve the efficiency of ISQE and verify the effectiveness of the proposed method in information security certification and accreditation through experiments.

1.3 Our Contributions

Although most of the work focuses on the formalization of ToE, selecting of security-critical components, and information evaluation algorithms. However, the work of formulating an efficient information evaluation model is not well studied. This paper proposes an ISQE model based on security-critical components (set) for CHISs, which is built upon analyzing and complementing the previous works. The main contributions of this paper are summarized as follows.

1) We propose an ISQE model based on security-critical components (set). This model includes formalizing the ToE based on security-critical components (set), calculating

information security quality value through quantitative evaluation algorithms, and determining security reinforcement strategy to make feedback adjustments. It can evaluate the information security quality of CHISs more efficiently.

2) The proposed recognition algorithm of security-critical components based on threat attack tree can help the formalization process of ToE. It mainly contains four steps: Asset mapping, topology construction, threat modeling, and importance ranking based on threat attack tree. It can help formalize the ToE and improve the efficiency of ISQE.
3) We consider the impact of different security-critical components (set) on ISQE. Moreover, we propose the measurement uncertainty 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 2 introduces the proposed ISQE model based on security-critical components (set). Section 3 explains the entire process of the evaluation model and verifies the validity of the algorithm using an example. Section 4 concludes and discusses the possible future research directions.

2 Proposed Model

Aiming at the problem of the lack of abstract description methods for CHISs, a recognition algorithm of security-critical components based on threat attack trees is proposed. Through formalization of security-critical components (set), an ISQE model based on security-critical components is proposed as shown in Fig. 2. Under the conditions of dynamic changes in the information system, the applicability and evaluation efficiency of the ISQE model can be improved, providing support for the construction of the information system security reinforcement strategies.

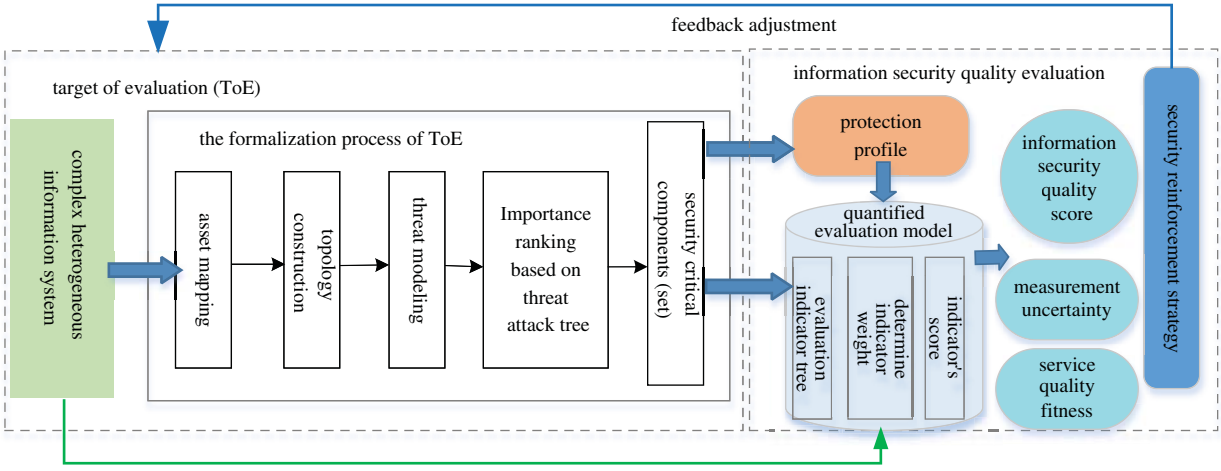

Figure 2: ISQE model based on security-critical components (set)

In the process of formalizing the ToE, the protection profile of the ToE is constructed through the selected security-critical components (set). The information security quality value is calculated based on the quantitative evaluation model. Meantime, compared with the evaluation results of the original information system that has not formalized the security-critical components (set), a novel indicator of measurement uncertainty is presented to measure the effectiveness of the model proposed in this paper.

2.1 The Recognition Algorithm of Security-Critical Components Based on Threat Attack Tree

Through the asset mapping of the selected ToE, the network topology diagram of its information system is constructed. And then, the threats faced by each asset is conducted based on threat modeling. If the threat to the asset is more serious, and the higher probability of the threat realized, the more important the asset affected by the threat. We calculate the security importance of the asset based on the probability of the threat using the vulnerability to successfully implement the attack, combined with the loss and impact caused by the threat. Security importance [28] is an indicator that measures the importance of the assets of the ToE in terms of security. According to the ranking comparison of the security importance of assets, the security-critical components (sets) of the ToE is established.

2.1.1 Asset Mapping

In the field of network security, the network infrastructure is the object to be protected, called assets. Assets are a highly abstract concept, referring to valuable objects, which may be tangible or intangible. Assets are not only the target of the attacker or the system resources that must be used to achieve the attack target, but also the things that the defender hopes to protect, such as passwords, personal identification information, data resources, and systems, software, firewalls, VPNs and other equipment that must be destroyed to achieve the goal. The model proposed in this paper mainly refers to tangible and valuable objects in the analysis.

In the process of asset mapping, assets and opened services are automatically obtained through multiple data acquisition methods such as active scanning and flow monitoring. Characteristics like asset fingerprint information, equipment type, and manufacturer are identified to construct asset files.

The asset file of CHIS covers four parts: Asset ownership, network asset type, asset attribute, and asset risk, as shown in Fig. 3. Through the establishment of asset files, sort out the network topology and asset details of the CHIS.

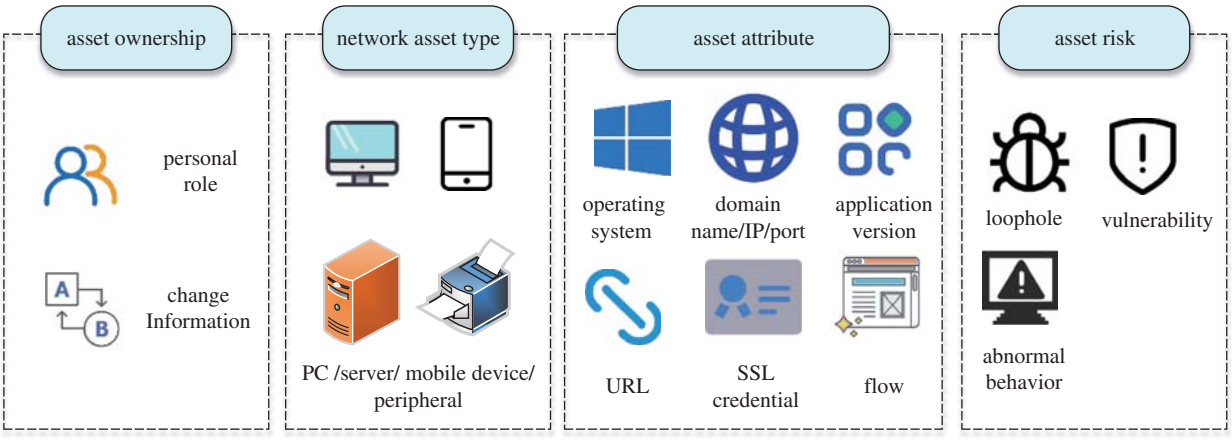

Figure 3: Asset file of complex heterogeneous information systems

2.1.2 Threat Modeling

The threat tree model is a graphical risk modeling method proposed by Schneire [34] in 1999, which is similar to the attack tree model. The threat tree model begins with a general

abstract description of all threats for a given ToE. The STRIDE threat model proposed by KOHNFELDER L and GARG P defines six general threats, which can be used to identify the root threat (RT) of each asset [35]. Among them, STRIDE stands for the acronym of six threats: spoofing identity, tampering with data, repudiation, data disclosure, denial of service (DoS), and elevation of privilege, respectively. The specific meaning of the STRIDE threat model is shown in Tab. 1.

Table 1: The STRIDE threat model

Threat category	Definition	The corresponding security attribute
Spoofing (S)	Impersonate other's identify	Identification
Tampering (T)	Tamper with data or code	Integrity
Repudiation (R)	Deny what has been done	Non-repudiation
Information disclosure (I)	Confidential information leakage	Confidentiality
Denial of service (D)	Denial of service	Availability
Elevation of privilege (E)	Unauthorized permission	Authorization

We use the STRIDE threat model to analyze each asset in a complex heterogeneous information system, analyze its threat attack tree, and identify the faced root threat (RT). Perform the second-level analysis of the RT to identify the attack threats it faces and mark it as ST_i $(i = 1, 2, \ldots, m; j = 1, 2, \ldots, n)$. Analyze the third-layer of attack threat ST_{ij}, identify the specific attack means to achieve ST_{ij}, and record it as a basic security event E_{ijk} $(i = 1, 2, \ldots, m; j = 1, 2, \ldots, n; k = 1, 2, \ldots, s)$. The basic security events are defined as independent events, that is, the relationship between the child nodes is logical OR. Using the STRIDE threat model to analyze assets is shown in Fig. 4.

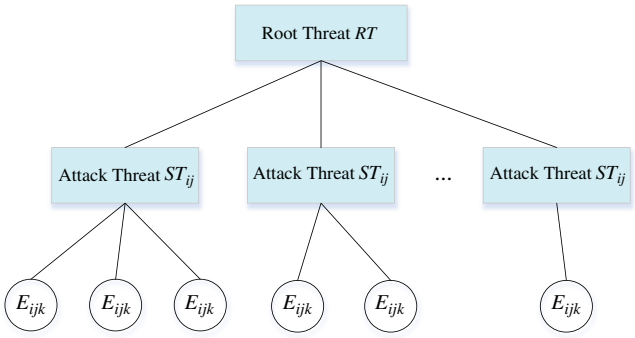

Figure 4: Threat modeling process

2.1.3 Importance Ranking Based on Threat Attack Tree

The security importance ranking based on the threat attack tree depends on the threat modeling of assets. Firstly, basic security events are determined based on the threat modeling situation. Then, we analyze the attack cost (AC) of the basic security event E_{ijk} to calculate the probability $P(E_{ijk})$ of its occurrence and then obtain the basic probability of the occurrence of

the attack threat $P(ST_{ij})$. Moreover, we calculate the safety importance of the asset by analyzing the severity of the loss of ST_{ij}.

In the calculation process of the probability $P(E_{ijk})$ of the occurrence of basic security events, it refers to the calculation method of attack potential against general products proposed in the information technology security assessment method CEM [36]. We evaluate the AC of basic security events from four indicators: attack time, equipment and facilities, professional technical capabilities, and data and access location, i.e., $AC(E_{ijk}) = \langle At, Eq, Pc, Al \rangle$, where At represents the time consumed by the attack, Eq represents the implementation level of the equipment, Pc represents the professional technical capability, and Al represents the data and access location. The efficiency numerical value of different indicators is shown in Tab. 2.

The weight vector $W = (w_1, w_2, w_3, w_4)$ of the above indicators is calculated by the Delphi method. It can also be calculated with other objective quantitative algorithms like the analytic hierarchy process (AHP) [37]. And then, the AC can be calculated by the following equation.

$$AC(E_{ijk}) = W \cdot U = (w_1, w_2, w_3, w_4) \cdot (u_1, u_2, u_3, u_4)^T \tag{1}$$

Table 2: The efficiency numerical values of different indicators

Attack time	Efficiency numerical values (u_1)	Equipment and facilities	Efficiency numerical values (u_2)	Professional technical capabilities	Efficiency numerical values (u_3)	Data and access location	Efficiency numerical values (u_4)
>3 months	5	Multiple custom equipment	5	Multiple experts	5	Very critical	5
<3 months	4	Custom equipment	4	Experts	4	Critical	4
<1 month	3	Professional equipment	3	Proficient	3	Sensitivity	3
<7 days	2	Standard equipment	2	Know	2	Limitation	2
<1 day	1	None	1	Nonprofessional	1	Public	1

The probability of occurrence of a basic security event is inversely proportional to its attack cost, that is, the lower the attack cost, the higher the probability of its occurrence. The calculation formula is as follows:

$$P(E_{ijk}) = \frac{1}{AC(E_{ijk})} \tag{2}$$

According to the occurrence probability of basic security events, the occurrence probability $P(ST_{ij})$ of ST_{ij} in the above-mentioned threat attack tree analysis is calculated. Due to the logical OR relationship between basic security events, the calculation formula for the probability of the occurrence threat ST_{ij} is as follows:

$$P(ST_{ij}) = \max\{P(E_{ij1}), P(E_{ij2}), \ldots, P(E_{ijk})\} \tag{3}$$

Analyze the severity of loss $Loss(S_{ij})$ caused by the threat ST_{ij}, and it also needs to be evaluated and assigned according to the Delphi method. The assignment range is 1 to 5. And then,

for each asset, according to the probability of occurrence of the threat ST_{ij} and the severity of the loss, the security importance is calculated. The formula is as follows:

$$M_i = \sum_{i=1}^{m} \sum_{j=1}^{n} P\left(ST_{ij}\right) \times Loss\left(ST_{ij}\right) \tag{4}$$

According to the sorting of the security importance degree M_i, the security-critical components (set) are identified.

2.2 *Information Security Quantitative Evaluation Algorithm Based on the Coefficient of Variation*

In order to better verify the effectiveness of the security-critical components (set) selection, it is reflected through the comparison of the ISQE results of the CHIS. We choose the information security quantitative evaluation algorithm based on coefficient variation to calculate the evaluation value.

Under the guidance of our country's information security standards, the specific indicator tree of ISQE for CHISs is made as shown in Fig. 5.

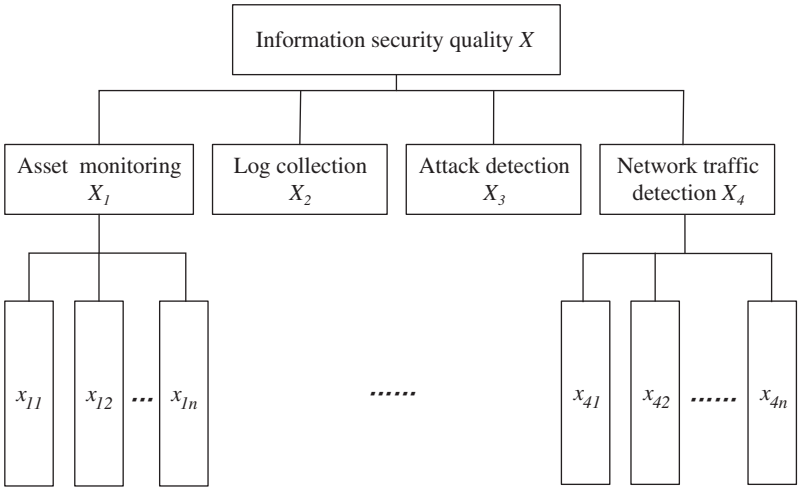

Figure 5: The specific indicator tree of ISQE for complex heterogeneous information systems

Where first-level indicators contain asset monitoring, log collection, attack detection, and network traffic detection, and second-level indicator marks as $X_i = \{X_{i1}, X_{i2}, \ldots, X_{in}\}$ $(i = 1, 2, \ldots, 4)$. The secondary indicators subordinate to asset monitoring include the number of security devices in the subnet, the types of services provided by each host in the subnet, and the types of operating systems of each host in the subnet. The secondary indicators of log collection include the number of alerts, frequency of bandwidth usage, and frequency of security incidents within the subnet. The secondary indicators of attack detection include four types of attack identification, which are port scan attack, distributed denial of service attack, brute force attack, and unknown attacks, respectively. The secondary indicators subordinate to network traffic detection include the average length of traffic, the average size of packets, the stream byte rate, the stream packet rate, and the proportion of abnormal traffic.

Step 1: Indicator normalization processing

Since the value ranges and dimensions of the collected assets, flow, vulnerability and other evaluation indicators are completely different. Then, we choose to use the more commonly dispersion standardization method to normalize indicators, the formula is shown below.

$$y_i = \frac{x_i - r_1}{r_2 - r_1}, \quad (i = 1, 2, \ldots, n) \tag{5}$$

Where x_i is the i-th secondary indicator, r_1 is the minimum value of the evaluation indicator, and r_2 is the maximum value of the evaluation indicator. Therefore, we can get a new sequence $y_1, y_2, \ldots, y_n \in [0, 1]$.

Step 2: Indicator weight determination

We choose the coefficient of variation algorithm to calculate the weight of the primary indicator and secondary indicator. Assuming there are k pieces of test data in total, each piece of data has n evaluation indicators, and then a $k \times n$ matrix is constructed, which is recorded as: $Y = (y_{ij})_{k \times n}$.

Firstly, the formula to calculate the average $\bar{y}_j$ of each indicator is as follows.

$$\bar{y}_j = \frac{1}{k} \sum_{i=1}^{k} y_{ij}, \quad (i = 1, 2, \ldots, k; j = 1, 2, \ldots, n) \tag{6}$$

Then, calculate the standard deviation S_j of each indicator, as shown in Eq. (7).

$$S_j = \sqrt{\frac{1}{k-1} \sum_{i=1}^{k} (y_{ij} - \bar{y}_j)^2}, \quad (i = 1, 2, \ldots, k; j = 1, 2, \ldots, n) \tag{7}$$

Therefore, the calculation formula of the coefficient of variation is as follows.

$$b_j = \frac{S_j}{|y_j|}, \quad (j = 1, 2, \ldots, n) \tag{8}$$

where the larger the value, the greater the degree of differentiation of the j-th indicator between different evaluation orders, and the greater the amount of information it can provide, so the indicator with violent fluctuations has a greater weight. So, the weight w_j of the j-th indicator is:

$$w_j = \frac{b_j}{\sum_{i=1}^{n} b_j}, \quad (j = 1, 2, \ldots, n) \tag{9}$$

Step 3: Building the indicator correlation function

According to the ISQE requirements and the actual situation of each evaluation indicator, we construct the corresponding correlation function [38]. All indicators can be roughly divided into three categories: positive indicator, negative indicator, and median indicator. The positive indicator refers to the indicator that the larger value indicates a safer system, and the reverse indicator is the opposite. The median indicator refers to the indicator that takes the middle value to indicate that the system is safer.

Therefore, the correlation function of the positive indicator is Eq. (10).

$$f(y)=\begin{cases} y, & 0\le y\le 1 \\ 0, & y<0 \ or \ y>1 \end{cases} \tag{10}$$

The correlation function of the negative indicator is as follows.

$$f(y)=\begin{cases} 1-y, & 0\le y\le 1 \\ 0, & y<0 \ or \ y>1 \end{cases} \tag{11}$$

The correlation function of the median indicator is as follows.

$$f(y)=\begin{cases} e^{\frac{(y-\alpha)^2}{2\sigma^2}}, & 0\le y\le 1 \\ 0, & y<0 \ or \ y>1 \end{cases} \tag{12}$$

where α and σ are determined according to the actual situation of specific evaluation indicators.

Step 4: Calculating the information security quality value

Under the condition of obtaining sufficient test data, we use the linear weighting algorithm to calculate the comprehensive information security quality value of the ToE. The calculation formula is as follows.

$$Score_{ISQE}=\frac{100}{n}\sum_{j=1}^{n} w_j \cdot f(y_i) \tag{13}$$

where $f(y_j)$ is the security quality value of the j-th indicator of the evaluation object, w_j is the weight of the indicator, and $Score_{ISQE}$ is the final security quality value of the ToE. The larger the value, the better the current system security situation.

2.3 Evaluation Indicators

According to the comparison of information security evaluation quality results, the novel indicator of measurement uncertainty is proposed to measure the effectiveness of the proposed evaluation model based on security-critical components. The calculation formula of measurement uncertainty is shown below.

$$\Delta\theta=\frac{\sum_{t=1}^{n}|Score_{ISQE\text{-}all}-Score_{ISQE\text{-}critical}|}{t} \tag{14}$$

where $Score_{ISQE\text{-}all}$ indicates ISQE results calculated from the data of all the components of the information system, $Score_{ISQE\text{-}critical}$ indicates ISQE results calculated from the data of security-critical components (set) of the information system, and t represents the running time of the system test. The closer the value of the above formula is to 0, the better.

3 Experimental Target and Results

We evaluate the proposed model through an example of the experimental environment we built in the laboratory and get the evaluation results.

3.1 Experimental Target

The experimental environment settings of the CHIS we constructed are shown in Fig. 6, including a managed node, a web server, a file server, a data server, a firewall, an attack machine, an intrusion detection system, and legitimate users.

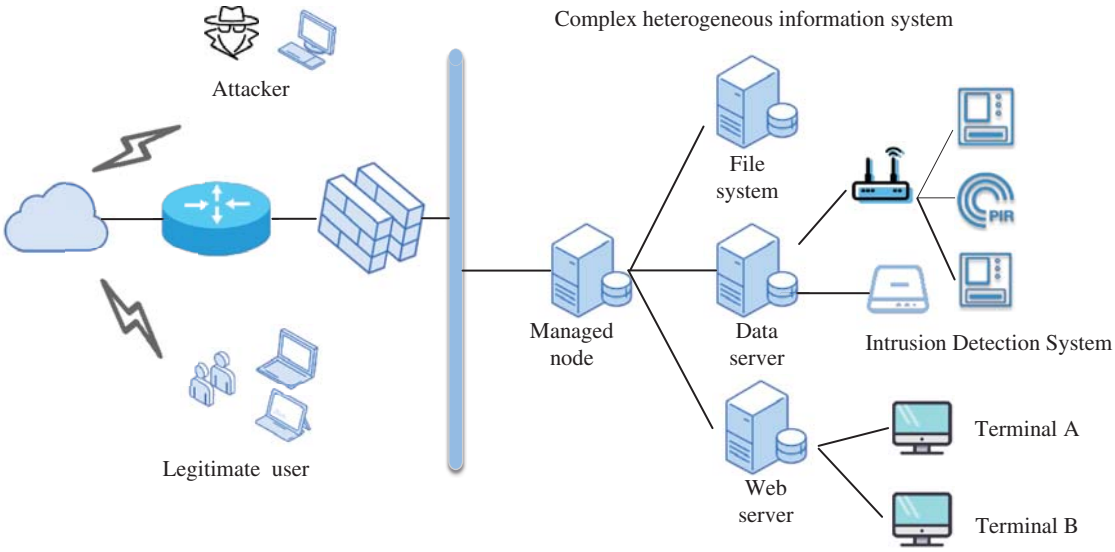

Figure 6: The experimental environment

The experiment uses the SYN Flood attack as the attack method to establish a large number of incomplete TCP connections with the server, making it unable to respond to normal service requests from legitimate users, thereby achieving denial of service. During the attack process, the information security quality value of the information system is gradually reduced by increasing the attack intensity. Threats are dealt with by deploying security management and control strategies. The information security quality value of the information system is evaluated according to the relevant indicator data obtained in each link of the system operation.

Specifically, we enter into two comparative trials. In the first set of experiments, we attacked the security-critical parts (sets) of the CHIS. In the other set of experiments, we attacked the non-security-critical parts (sets) of the CHIS. Compare the differences between the global ISQE results and the partial evaluation results with security-critical components in the two experiments.

3.2 Experimental Results

3.2.1 Identify the Assets and Build the Topology of ToE

The simulation experiment focuses on the impact of the selection and construction of security-critical components (set) on the evaluation of information security quality. Due to the network topology and asset identification of the CHIS have been completed based on the establishment of an experimental environment, the asset list has been formed. The asset identification granularity of CHISs is determined by the analyst, and this paper only focuses on the device level. A total of eight assets are identified, which are system entrance gateway, system entrance firewall, management node server, data server, web server, file system server, and terminals.

3.2.2 Construct the Security-Critical Components

We perform threat tree attack analysis for each asset. Root threats are identified using the STRIDE model among them. It further identified the attack threats ST against the CHIS, namely access control destruction ST_1, semi-invasive attacks ST_2, invasive attacks ST_3, and environmental attack ST_4. Then, in terms of the attack threat ST, we further identify the 14 basic security events that realize the attack and draw a threat attack tree for each asset, as shown in Figs. 7, 8.

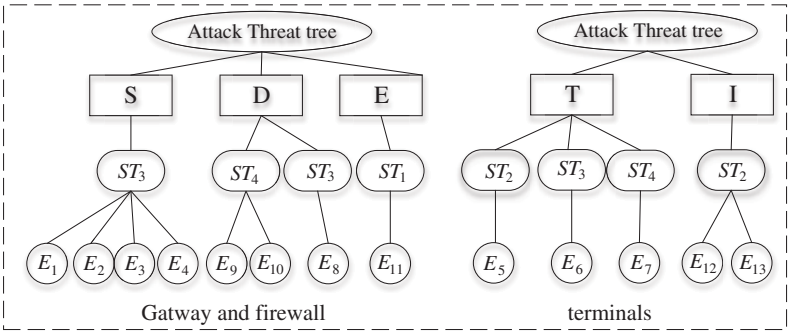

Figure 7: Threat attack tree analysis of gateway and terminals

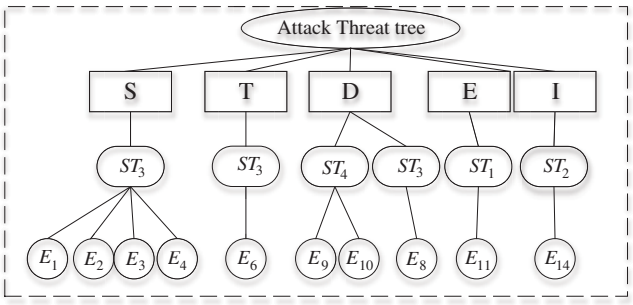

Figure 8: Threat attack tree analysis of managed node, web server, data server, and file system server

When analyzing the attack cost (AC) of basic security events, we mark and assign weights to the four elements $\langle At, Eq, Pc, Al\rangle$ based on the Delphi method firstly. According to Eqs. (1) and (2), we calculate the probability of occurrence of basic security events as shown in Tab. 3.

The basic security events under the threat of spoofing and denial of service have higher requirements for equipment and professionals, so the weight is assigned to $w_{Eq} = 0.3$, $w_{Pc} = 0.3$, $w_{At} = 0.2$ and $w_{Al} = 0.2$. The basic security events under the threat of elevation of privilege and tampering with data are highly dependent on professionals and access locations, so in terms of weight assignment, $w_{Pc} = 0.3$, $w_{Al} = 0.3$, $w_{At} = 0.2$ and $w_{Eq} = 0.2$. As for the basic security events under information disclosure, the requirements for professionals are the highest. Under this condition, we set the weight of the quadruple as $w_{Pc} = 0.4$, $w_{Al} = 0.3$, $w_{Eq} = 0.2$ and $w_{At} = 0.1$.

Table 3: The list of basic security events and the probability of occurrence

Serial number	Basic security event	The probability of occurrence
1	Account key leaked	0.357
2	Username brute force enumeration	0.323
3	Weak password	0.385
4	Identity forgery and attacks (such as SQL injection, etc.)	0.333
5	Channel attack	0.286
6	Database data tampering	0.263
7	Terminal data tampering	0.333
8	Denial of service attack	0.417
9	Abnormal equipment room	0.370
10	Abnormal power supply system	0.370
11	Access control destruction	0.286
12	Terminal data is not encrypted	0.357
13	The communication network lacks dynamic authentication	0.3125
14	Database clear text transmission	0.270

Based on Eq. (3), we can calculate the probability of threat ST_{ij}. Through analyzing the severity of loss $Loss\left(S_{ij}\right)$ caused by the threat ST_{ij}, the security importance degree M_i of different assets can be calculated by Eq. (4). The security importance ranking result is shown in Tab. 4.

Table 4: The security importance ranking result

Asset	Security importance	Asset	Security importance
Management node server	6.112	System entrance gateway	4.243
File system server	6.112	System entrance firewall	4.243
Web server	6.112	Terminal A	3.647
Data server	6.112	Terminal B	3.647

We choose 4 as the threshold for the security importance ranking. So, the content of constructed security-critical components (set) is management node server, file system server, web server, data server, system entrance gateway, and system entrance firewall.

3.2.3 Comparison of ISQE Results

In the first set of experiments, we attacked the web server. And in the other set of experiment, we attaced the terminal B of the CHIS to get the experimental results as shown in Figs. 9 and 10.

The measurement uncertainty can be calculated by Eq. (14), i.e., $\Delta\theta_1 = 3.6413$ and $\Delta\theta_2 = 7.875$.

Through the analysis of the experimental results, it can be known that when attacking different parts of the CHIS, the information security evaluation model based on security-critical components (set) proposed in this paper can perform better system security quality evaluation.

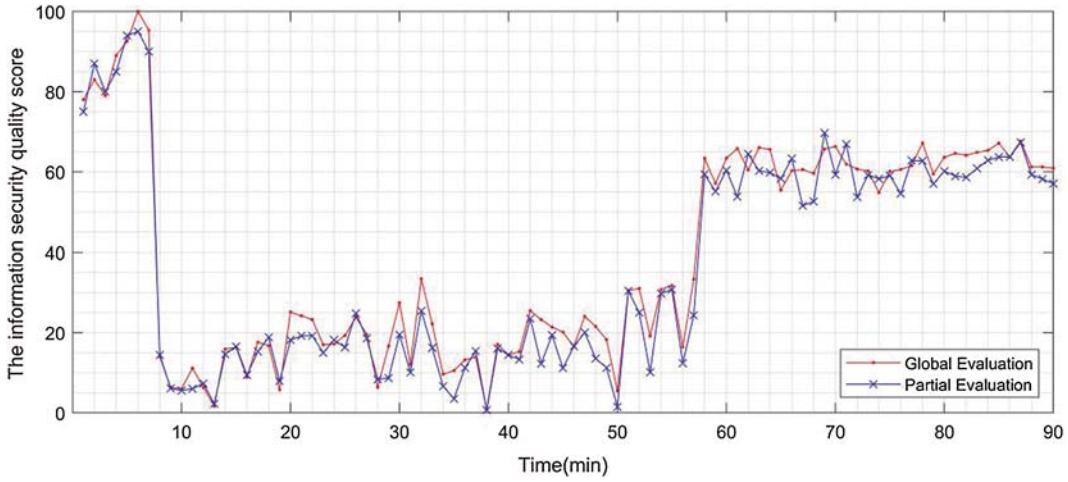

Figure 9: Comparison of the results of attacking security-critical components (set)

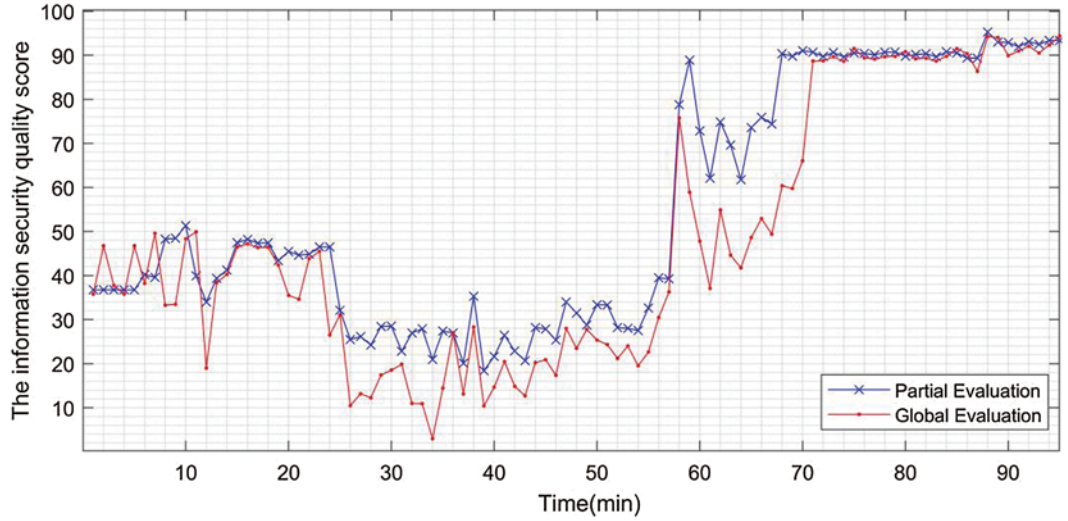

Figure 10: Comparison of the results of attacking non-security-critical components (set)

4 Conclusion

The efficiency of ISQE hinders the update of security reinforcement strategies for CHISs. To solve the problem that there is a lack of an efficient evaluation model, this paper proposes an ISQE model based on security-critical components (set) to quantify the $Score_{ISQE}$ of the CHIS. The evaluation model includes three modules, (1) the core security-critical components (set) identification process based on threat attack tree, (2) the quantitative evaluation process based on the coefficient of variation algorithm, (3) the evaluation indicator of measurement uncertainty to supervise the validity of the proposed model. Also, our research provides ideas for the efficient implementation of information security certification and accreditation for information systems.

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 the National Key R&D Program of China under Grant 2019YFB2102400, 2016YFF0204001, 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

[1] A. Sun, G. Gao, T. Ji and X. Tu, "One quantifiable security evaluation model for cloud computing platform," in *Proc. CBD*, Lanzhou, China, pp. 197–201, 2018.

[2] J. Shen, T. Q. Zhou, D. B. He, Y. X. Zhang, X. M. Sun *et al.,* "Block design-based key agreement for group data sharing in cloud computing," *IEEE Transactions on Dependable and Secure Computing*, vol. 16, no. 6, pp. 996–1010, 2019.

[3] A. Roukounaki, S. Efremidis, J. Soldatos, J. Neises, T. Walloschke *et al.,* "Scalable and configurable end-to-end collection and analysis of IoT security data: Towards end-to-end security in IoT systems," in *Proc. GIoTS*, Aarhus, Denmark, pp. 1–6, 2019.

[4] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum and N. Ghani, "Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2702–2733, 2019.

[5] O. A. Bubareva, "Ontology integration in complex information systems with distributed architecture," in *Proc. EDM*, Erlagol, Russia, pp. 212–215, 2018.

[6] J. Li, D. L. Zhao, B. F. Ge, J. Jiang and K. W. Yang, "Disintegration of operational capability of heterogeneous combat networks under incomplete information," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 88, pp. 1–8, 2018.

[7] T. Y. Wang, Z. F. Xie and B. Gao, "Design of distributed heterogeneous general signal processing platform architecture," in *Proc. ICSIDP*, Chongqing, China, pp. 1–4, 2019.

[8] W. Han, Z. Tian, Z. Huang, L. Zhong and Y. Jia, "System architecture and key technologies of network security situation awareness system yhsas," *Computers, Materials & Continua*, vol. 59, no. 1, pp. 167–180, 2019.

[9] P. Oser, S. Feger, P. W. Woźniak, J. Karolus, D. Spangnuelo *et al.,* "SAFER: Development and evaluation of an iot device risk assessment framework in a multinational organization," *Proc. of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 4, no. 3, pp. 1–22, 2020.

[10] N. Bu, "The implementation process of our country's information security product certification system," *China Quality Certification*, vol. 2, pp. 32–33, 2012.

[11] R. N. Akram, K. Markantonakis, K. Mayes, O. Habachi, D. Sauveron *et al.,* "Security, privacy and safety evaluation of dynamic and static fleets of drones," in *Proc. DASC*, St. Petersburg, FL, USA, pp. 1–12, 2017.

[12] J. Howell, "Number of connected IoT devices will surge to 125 billion by 2030," Beijing, China, 2020. [Online]. Available: https://technology.ihs.com/596542/.

[13] O. Alrawi, C. Lever, M. Antonakakis and F. Monrose, "SoK: Security evaluation of home-based IoT deployments," in *Proc. SP*, San Francisco, CA, USA, pp. 1362–1380, 2019.

[14] J. Zhang, H. J. Chen, L. Y. Gong, J. Cao and Z. J. Gu, "The current research of IoT security," in *Proc. DSC*, Hangzhou, China, pp. 346–353, 2019.

[15] Z. Baig and S. Zeadally, "Cyber-security risk assessment framework for critical infrastructures," *Intelligent Automation & Soft Computing*, vol. 25, no. 1, pp. 121–129, 2019.

[16] B. Che, L. Liu and H. Zhang, "KNEMAG: Key node estimation mechanism based on attack graph for IOT security," *Journal of Internet of Things*, vol. 2, no. 4, pp. 145–162, 2020.

[17] G. Yang, M. Yang, S. Salam and J. Zeng, "Research on protecting information security based on the method of hierarchical classification in the era of big data," *Journal of Cyber Security*, vol. 1, no. 1, pp. 19–28, 2019.

[18] C. Qian, X. Li, N. Sun and Y. Tian, "Data security defense and algorithm for edge computing based on mean field game," *Journal of Cyber Security*, vol. 2, no. 2, pp. 97–106, 2020.

[19] J. R. B. Higuera, J. B. Higuera, J. A. S. Montalvo, J. C. Villalba and J. J. N. Pérez, "Benchmarking approach to compare web applications static analysis tools detecting owasp top ten security vulnerabilities," *Computers, Materials & Continua*, vol. 64, no. 3, pp. 1555–1577, 2020.

[20] P. Centonze, "Security and privacy frameworks for access control big data systems," *Computers, Materials & Continua*, vol. 59, no. 2, pp. 361–374, 2019.

[21] J. P. Gao, S. S. Shi, W. Jia and F. Wang, "The revision status of common criteria," *Information Technology & Standardization*, vol. 5, pp. 64–67, 2018.

[22] Z. Q. Wang, "Study on manufacturing quality control of hinge parts," M.S. Thesis, Inner Mongolia Agricultural University, Hohhot, Inner Mongolia, China, 2009.

[23] Y. Xu, "Research and implementation in key components tracking technology of common-rail pipe automatic assembly line and economic," M.S. Thesis, Nanchang University, Nanchang, Jiangxi, China, 2019.

[24] J. J. Lv, "Design and analysis of key parts of top drive system of vehicle mounted drilling rig," *Coal Mine Machinery*, vol. 38, no. 3, pp. 78–80, 2017.

[25] L. Sun, "Identification method of key parts and important parts of military enterprise model products," *China Quality Certification*, vol. 12, pp. 56–57, 2016.

[26] X. Shi, C. Wang and C. Liu, "Analysis on the management of U.S. military aviation critical safety items and suggestions on domestic status quo," *Aeronautic Standardization & Quality*, vol. 4, pp. 46–49, 2020.

[27] J. Sheng, H. Wu and Z. Huang, "Recognition of the software key component based on the characteristic index fault forest model," *Fire Control & Command Control*, vol. 35, no. 12, pp. 171–176, 2010.

[28] W. Q. Tao, J. Y. Zhang and Q. M. Chen, "Research on recognition of security key component of IT products based on threat trees," *Information Technology and Network Security*, vol. 38, no. 3, pp. 4–8, 2019.

[29] Knownsec, "Zoomeye, China," 2020. [Online]. Available: https://www.zoomeye.org/component.

[30] A. Qi, "Global eagle cloud situation is based on data service wall chart to improve situation awareness," China, 2020. [Online]. Available: https://www.qianxin.com/news/detail?news_id=705.

[31] Shodan, "The search engine for the internet of things," China, 2020. [Online]. Available: https://www.shodan.io/.

[32] F. H. Li, "The design and implementation of network equipment identification system," M.S. Thesis, Beijing University of Posts and Telecommunications, Beijing, China, 2017.

[33] W. C. Yang, Y. B. Guo, T. Li and B. Q. Zhu, "Method based on traffic Fingerprint for IoT device identification and IoT security model," *Computer Science*, vol. 47, no. 7, pp. 299–306, 2020.

[34] B. Schneire, "Attack trees: Modeling security threats," *Dr Dobb's Journal*, vol. 24, no. 12, pp. 21–29, 1999.

[35] S. Adam, "Threat modeling, design and delivery of more secure software," China: Machinery Industry Press, 2015. [Online]. Available: https://max.book118.com/html/2018/0802/6025012233001210.shtm.

[36] CCMB-2017-04-004, "Common methodology for information technology security evaluation," China, 2020. [Online]. Available: http://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1%EF%BC%B25.pdf.

[37] J. Zhao, R. Wang, Z. M. Li, M. Lei and M. Y. Ma, "Security threats and risk assessment of IoT system," *Journal of Beijing University of Posts and Telecommunications*, vol. 40, pp. 135–139, 2017.

[38] P. Lv, X. L. Wang, H. L. Yv, C. Wang and C. X. Liu, "Dynamical and scalable evaluation model for dam seepage safety based on FDA," *Journal of Hohai University (Natural Sciences)*, vol. 5, pp. 433–439, 2020.