IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 13 February 2023, accepted 2 March 2023, date of publication 6 March 2023, date of current version 8 May 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3253393

RESEARCH ARTICLE

Cybersecurity Status Assessment of Cloud Manufacturing Systems Based on Semiquantitative Information

SHIMING LI[1], XINGSHUO XU[1], GUOHUI ZHOU[1], YUHE WANG[1], ZHICONG LI[1], YAN ZHAO[2], AND WEIQI ZHAO[3]

[1]College of Computer Science and Information Engineering, Harbin Normal University, Harbin 150025, China
[2]School of Information Technology, Luoyang Normal University, Luoyang, Henan 471934, China
[3]School of Computer Science and Technology, Jilin University, Changchun 130000, China

Corresponding authors: Yuhe Wang (cs2008wyh@163.com), Zhicong Li (lizhicong72@163.com), and Yan Zhao (zhao_yan22@163.com)

This work was supported in part by the Provincial Universities Basic Business Expense Scientific Research Projects of Heilongjiang Province under Grant 2021-KYYWF-0179, in part by the Science and Technology Project of Henan Province under Grant 212102310991, in part by the Key Scientific Research Project of Henan Province under Grant 21A413001, and in part by the Postgraduate Innovation Project of Harbin Normal University under Grant HSDSSCX2021-121.

ABSTRACT The network security status assessment (NSSA) method can evaluate the network security status of cloud manufacturing systems (CMSs), which is of great significance to reduce the network security risk and loss of CMSs. At present, the NSSA of CMSs suitable for semiquantitative and uncertain information conditions is commonly used, which has certain limitations and low accuracy. This paper proposes an NSSA method for CMSs based on semiquantitative information. First, through the detailed analysis of the influencing factors of the network security status of the CMSs, the security evaluation indicators are selected, and the evaluation framework containing multilevel indicators is established by combining semiquantitative information. Second, the evaluation level is established according to the data distribution and the properties of the indicators. Third, a process of data fusion reasoning based on an evidential reasoning algorithm is designed, and a strong reference fusion case is given. Finally, the effectiveness of the proposed security state assessment algorithm in the NSSA of CMSs is verified and analyzed by simulation experiments. The experimental results show that the proposed method can make full use of semiquantitative information and uncertain information to evaluate the network security status of CMSs, and the evaluation results can reflect the actual security status of CMSs.

INDEX TERMS Cloud manufacturing systems (CMSs), network security status assessment (NSSA), evidential reasoning (ER), semiquantitative information, condition evaluation.

I. INTRODUCTION

Cloud manufacturing (CM) is a new model of networked manufacturing based on knowledge and resource sharing, aiming at low energy consumption and high efficiency production and integrating cloud computing, intelligent manufacturing, Internet of Things (IoT), high performance computing, and intelligent information processing technologies for service-oriented applications, which has attracted international attention in recent years [1]. Due to the high openness of CM, the cloud manufacturing system (CMS), the core part of CM, is highly dependent on the Internet, IoT and cloud computing. At the same time, the security of the CMS itself is also highly risky and even determines the security of CM [2].

At present, although there are few public reports on CM network security incidents in the world, there are many network security incidents and serious losses or threats in the manufacturing field closely related to CM. For example, in 2019, the Bitcoin ransomware attack on Pilz, a maker of automated tools, disrupted its network services. In 2020, German silicon wafer manufacturer X-FAB was attacked

The associate editor coordinating the review of this manuscript and approving it for publication was Ali Kashif Bashir.

by a network virus and forced to shut down some of its manufacturing plants. In 2021, Colonial Pipeline, a US refined product pipeline operator, suffered a ransomware attack and was forced to shut down the company's critical fuel network, among others. According to the relevant research reports of the International Data Organization, the network security maintenance of cloud manufacturing systems (CMSs) plays an important role in their stable operation [3]. The security of CMS is very important and has become an important issue restricting the development of CM.

Because the CMS has the characteristics of high complexity and high heterogeneity after integrating various advanced technologies, its own security maintenance is very important, especially the network security protection of the CMS, which is a difficult problem [4]. To do a good job in the security protection of CMSs, it has become very important and meaningful work to accurately evaluate the network security status of the system beforehand because it can let security maintenance personnel know the security status of the CMS in advance to predict the security risk and implement the security protection deployment of the system in advance to avoid or reduce the risk of being violated as much as possible. To reduce the loss after damage, preassessment of the security state of the system is not only becoming increasingly important but also has a higher status [5], [6].

The so-called network security assessment of CMS evaluates different types of network security status information of CMS by using some algorithm and determines the network security assessment results according to the evaluation algorithm results and the network security level of CMS formulated in advance [7], which provides an important reference for network security managers to effectively protect CMS. Thus, the risk of damage can be minimized, and the network security protection capability of CMSs can be improved [8].

At present, the network security evaluation methods used in various fields can be roughly divided into evaluation methods based on expert knowledge [9] and evaluation methods based on data-driven methods [10].

The evaluation methods based on expert knowledge mainly include the hierarchical evaluation method, the evaluation method based on Dempster-Shafer (D-S) evidence theory and the hidden Markov evaluation method. Among them, the hierarchical evaluation method can comprehensively use qualitative knowledge and quantitative information to improve the accuracy of the evaluation results [11], and it can be used in the industrial IoT cloud system to evaluate from multiple perspectives. The evaluation method based on D-S evidence theory not only has the function of hierarchical evaluation but can also deal with all kinds of uncertain and conflicting information [12]. The hidden Markov evaluation method can evaluate and dynamically describe the network security status in real-time and provide timely responses [13]. However, the above methods have many shortcomings due to excessive reliance on expert knowledge and human subjectivity. For example, the lack of experience of expert knowledge may directly lead to the serious deviation of evaluation results from the true value, and when incomplete information and semiquantitative information are involved, accurate evaluation results cannot be obtained, and even the computational complexity is increased in vain [14].

Data-driven evaluation methods include the Bayesian inference analysis method and machine learning-based evaluation method. The former uses prior knowledge to obtain conclusions by statistical sample information, which can address uncertain problems [15]. Then, knowledge reasoning is used to solve the problem, which can accurately identify network attacks and comprehensively and flexibly evaluate network security conditions [16]. However, the evaluation method based on data-driven methods cannot deal with semiquantitative information, the demand for evaluation data is large, the quantitative information evaluation results of small-scale samples are not accurate, and the accurate results need to be repeatedly trained, which not only increases the difficulty of training but also has the problem that the optimization principle of model training cannot be explained. Although expert knowledge can compensate for the lack of model training, it will not improve the evaluation accuracy, so it cannot reflect the real advantages of expert knowledge [17].

The existing network security evaluation methods mainly have the following shortcomings:

(1) Some methods cannot process semiquantitative information, or the computational complexity is too high when processing semiquantitative information.

(2) Some methods strongly rely on expert knowledge or human subjectivity, which cannot effectively use expert knowledge and even seriously affect the accuracy of the evaluation results.

(3) Some methods cannot accurately deal with uncertain information in the evaluation process.

In summary, this paper proposes a network security status assessment (NSSA) method for CMS based on semiquantitative information, which can comprehensively use qualitative knowledge and quantitative information to fuse different types of data and can also express the uncertainty information of various security assessment indicators in CMS. According to the state data of the CMS, a new security state evaluation framework is established, and the network security level of the CMS is evaluated by referring to the national network security evaluation level standard.

II. PROBLEM DESCRIPTION

The cyber risk of CMS is the degree of impact on the interests of individuals, organizations or countries due to potential threats or with a certain probability. The judgment of the degree is often determined according to the loss characteristics. Assessing the cyber risk of CMS in advance can find and solve problems as early as possible before the

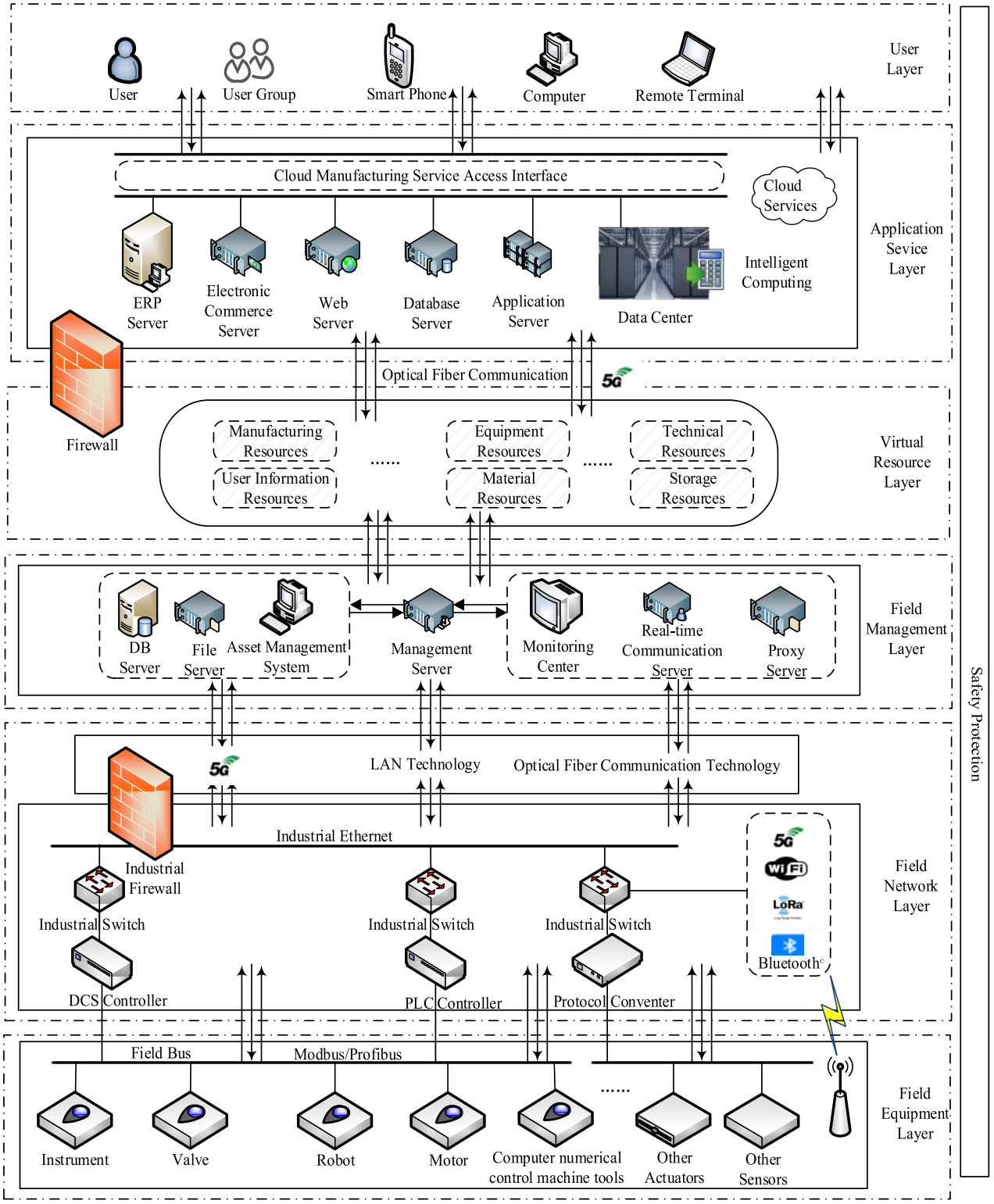


FIGURE 1. CMS framework.

production of CMS and maximize the network security of the system. The CMS model involved in this paper is shown in Fig. 1.

In Fig. 1, because the field equipment layer is mostly all kinds of sensors, digital machine tools, mechanical devices, instruments, etc. At the same time, the incompatibility

between various industrial protocols further aggravates the heterogeneity of data.

In Fig. 1, the field network layer is based on industrial Ethernet and uses various wireless communication technologies to realize the transmission of industrial data and instructions. Field management mainly realizes the management function of equipment, production, data, documents and assets within the manufacturing enterprise. The application service layer is mainly oriented to cloud services and uses the cloud platform to connect multiple CMSs. The user layer is mainly for individuals, organizations, governments, ecological enterprises and other users to access the CMS to complete mutual coordination and customization services.

The heterogeneity of the whole CMS structure increases the complexity of the system. When the industrial system that used to be an ''isolated island'' is connected to the cloud platform, it is bound to cause people's concern about its security. Since different levels in Fig. 1 involve different technologies and the security issues among the technologies are complex, this paper analyzes and evaluates the security status of CMS from a data perspective.

Due to the large differences in equipment, protocols, working principles and technologies of each layer, the dynamic data of each layer also have different attributes and characteristics, and the data itself can reflect the network security status of this layer to varying degrees. Therefore, the network security status of the CMS can be evaluated by analyzing the data of each layer of the CMS and scientifically selecting the core attribute data and indicators.

There is a large amount of semiquantitative information in the CMS, and it can reflect the correlation, constraints, fuzziness and uncertainty among the data of the network security status, which will increase the difficulty of assessment [18]. Therefore, the evaluation method itself should have the ability to comprehensively use semiquantitative information and deal with various uncertain information [19].

III. RELATED TECHNOLOGIES

A. SEMI-QUANTITATIVE INFORMATION

Semiquantitative information refers to the information that contains quantitative data and qualitative knowledge. Quantitative data refer to the specific data that can be expressed as a certain amount or range, and they can be directly obtained by monitoring equipment. Qualitative knowledge is subjective and abstract information that cannot be measured or collected and can only be acquired by expert knowledge through the evaluation and perception of complex systems [20].

B. ER ALGORITHM

The evidential reasoning (ER) algorithm is a method to fuse multisource information based on decision theory and the Dempster combination rule in D-S evidence theory, which is suitable for dealing with semiquantitative information and various uncertain information [21]. Compared with D-S evidence theory, the linear calculation process of the ER algorithm can not only reduce the computational complexity but also solve the conflict problem between evidence attributes [22]. At present, the ER algorithm has been applied in typical applications. For example, Zhou et al. applied it to oil pipeline leakage fault monitoring [23], Qiu et al. applied it to relay fault diagnosis [24], Bi et al. applied it to weapon equipment system effectiveness evaluation [25], and it was applied to relay fault diagnosis. Wang et al. applied it to the safety assessment of natural gas storage tanks [26]. In addition, the ER algorithm has significant advantages when evaluating the network security status of CMS fusing a large number of different types of information. The detailed steps of the ER algorithm are described in [27] as follows:

It is assumed that there are basic attributes $\{\gamma_1, \gamma_2, \ldots, \gamma_i, \ldots, \gamma_M\}$ constituting a multilevel evaluation system, where $\{\omega_1, \omega_2, \ldots, \omega_i, \ldots, \omega_M\}$ represents the weight of the basic attribute, and $0 \leq \omega_i \leq 1$. The output is rated N. Then, the basic steps of the ER algorithm are as follows:

(1) After the value of the evaluation attribute is determined, it is necessary to calculate the corresponding confidence degree to obtain the basic probability quality. As shown in Formula (1).

$$\begin{cases} \beta_{i,j} = \dfrac{R_{i,j+1} - U(r_i)}{R_{i,j+1} - R_{i,j}}, \ R_{i,j} \leq U(r_i) \leq R_{i,j+1} \\ \beta_{i,j+1} = 1 - \beta_{i,j} \\ \beta_{i,k} = 0, k = 1, \ldots, N, k \neq j, j+1. \end{cases} \tag{1}$$

where $U(r_i)$ represents the value of attribute r_i, and $R_{i,j}$ represents the reference value of attribute r_i at the j evaluation level.

(2) Convert confidence into a basic probability mass, as shown in formulas (2) $\sim$ (5).

$$P_{i,j} = \omega_i \beta_{i,j} \tag{2}$$

$$P_{i,\theta} = 1 - \omega_i \sum_{j=1}^{N} \beta_{i,j} \tag{3}$$

$$\overline{P_{i,\theta}} = 1 - \omega_i \tag{4}$$

$$Q_{i,\theta} = \omega_i \left(1 - \sum_{j=1}^{N} \beta_{i,j} \right) \tag{5}$$

where $P_{i,j}$ represents the basic probability quality relative to the evaluation level j, $P_{i,\theta}$ represents the basic probability setting of the evaluation set of i that is, the residual probability attribute without the i basic attribute of the assigned result, $P_{i,\theta} = Q_{i,\theta} + \overline{P_{i,\theta}}$. $Q_{i,\theta}$ represents the unassigned basic probability mass with respect to the incompleteness of the i-th fundamental attribute, and $\overline{P_{i,\theta}}$ represents the unassigned basic probability mass with respect to the insignificance of the i-th fundamental attribute.

(3) The probability quality of the j valuation level can be obtained by combining the first i basic attributes with

evidence theory. The steps are shown in formulas (6) ∼ (9).

$$P_{I(i+1),j} = K_{I(i+1)}[P_{I(i),j}P_{i+1,j} + P_{I(i),j}P_{i+1,\theta} + P_{I(i),\theta}P_{i+1,j}] \tag{6}$$

$$P_{I(i),\theta} = \overline{P_{I(i),\theta}} + Q_{I(i),\theta} \tag{7}$$

$$Q_{I(i+1),\theta} = K_{I(i+1)}[Q_{I(i),\theta}Q_{i+1,\theta} + Q_{I(i),\theta}\overline{P_{i+1,\theta}} + \overline{P_{I(i),\theta}}Q_{i+1,\theta}] \tag{8}$$

$$\overline{P_{I(i+1),\theta}} = K_{I(i+1)}\left[\overline{P_{I(i),\theta}P_{i+1,\theta}}\right] \tag{9}$$

where $P_{I(i),j}$ represents the probability quality of the j evaluation level after the combination of the first i basic attributes. It can be obtained by the following formula (10).

$$K_{I(i+1)} = \frac{1}{1 - \sum_{k=1}^{N}\sum_{\substack{j=1 \\ j\neq k}}^{N} P_{I(i),k}P_{i+1,j}} \tag{10}$$

(4) Based on the obtained probability quality, the confidence degree σ_j of the j-th evaluation level and the residual confidence degree σ_θ of the unset evaluation result are calculated, as shown in formula (11) and formula (12).

$$\sigma_j = \frac{P_{I(M),j}}{1 - \overline{P_{I(M),\theta}}},\ j = 1, 2, 3, \ldots, N. \tag{11}$$

$$\sigma_\theta = \frac{Q_{I(M),\theta}}{1 - \overline{P_{I(M),\theta}}} \tag{12}$$

The above are the basic steps of the ER algorithm.

IV. NSSA FRAMEWORK OF CMS

To solve the problem of the NSSA of CMSs, this paper proposes an NSSA method for CMSs based on semiquantitative information. The system network security status data are analyzed quantitatively and qualitatively, and then the ER algorithm is used to fuse the data step by step, compare the results with the predefined level division, and finally determine the assessment result of the CMS.

To facilitate the description of the framework evaluation process of this paper, the field management layer and the field device layer are selected from Fig. 1 for evaluation, and each layer constructs an evaluation indicator system from three aspects: equipment security, service quality and network security.

(1) Select evaluation indicators. In the process of selecting evaluation indicators, it is necessary to ensure that the selected indicators can objectively reflect the real network situation of the CMS and meet the relevant requirements of system security to ensure the availability of the selected indicators. Evaluation indicators can be divided into two categories: one category of indicators is quantitative data, and the other category of indicators is qualitative knowledge. To improve the accuracy of the evaluation, first, according to the specific objects involved in each layer of the CMS, the important and typical core indicators are scientifically analyzed and selected to construct the evaluation framework. The qualitative indicators are then quantified to make them available for quantitative analysis.

To facilitate the description of the framework evaluation process of this paper, the field management layer and the field device layer are selected from Fig. 1 for evaluation, and each layer constructs an evaluation indicator system from three aspects: equipment security, service quality and network security.

Assume that Y is the overall indicator set reflecting the network security status of the CMS, which is defined as $Y = [y_1, \ldots, y_M]^T$. The network security status of CMS is evaluated from three dimensions: network equipment security, service quality and network security. Assume that set y is the security evaluation indicator of network equipment, which is defined as $y = [y^1, \ldots, y^L]^T, y \subseteq Y$; Set e is the service quality evaluation indicator, which is defined as $e = [y^1, \ldots, y^N]^T, e \subseteq Y$; Set g is the network security evaluation indicator, which is defined as $g = [y^1, \ldots, y^G], g \subseteq Y$; and $L \leq M, N \leq M, G \leq M$.

2) Establish an evaluation framework.

The NSSA indicators in CMS are related to each other. When improving the accuracy of assessment results, we cannot just rely on the method of processing a single piece of information but comprehensively consider and reasonably use semiquantitative information to build a more accurate assessment framework.

3) Establish a model to evaluate the network security status of the CMS. Its model construction is shown in Equation (13).

$$\begin{cases} D(t) = \varpi(e(t)) \\ Q(t) = \varpi(y(t)) \\ R(t) = \varpi(g(t)) \\ O(t) = \varpi(D(t), Q(t), R(t)) \end{cases} \tag{13}$$

Table 1 shows the meanings of specific parameters in Formula (13).

A. EVALUATION METRICS

The evaluation indicators are divided into quantitative indicators and qualitative indicators, and each indicator takes into account all kinds of current standards as much as possible according to the specific circumstances. CMS has the characteristics of high complexity and low security due to its network heterogeneity, component diversity, high confidentiality and high added value of commercial big data. Its centralized storage makes CMS more likely to become a high-risk area of network attacks.

By selecting reasonable security indicators that meet the evaluation requirements to evaluate the network security status of the CMS, it can understand its own security level and risk level and warn security managers in time.

In this paper, the network security status evaluation indicators of CMS are selected from the three dimensions of equipment security, service quality and network security.

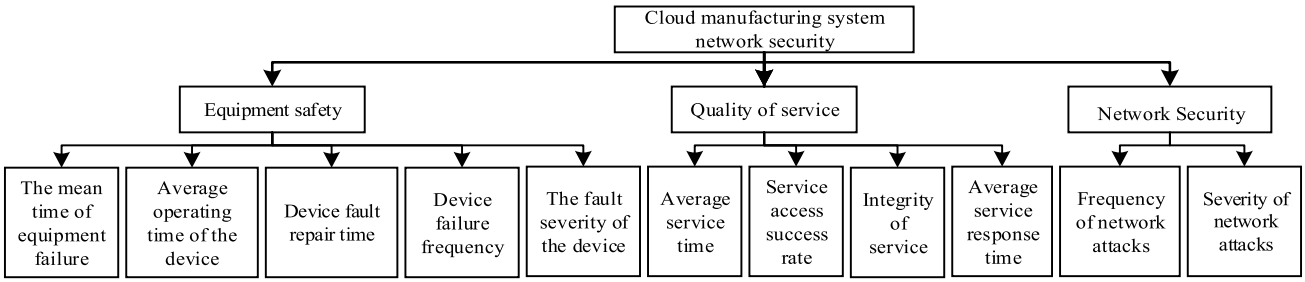


FIGURE 2. Evaluation indicator system structure.

TABLE 1. The meaning of the parameters.

No.	Parameters	Meaning
01	$e(t)$	the service quality evaluation indicator data at the time t
02	$y(t)$	the Network device security evaluation indicator data at the time t
03	$g(t)$	the network security evaluation indicator data at the time t
04	$\varpi(\bullet)$	the Nonlinear function, ER algorithm for data fusion
05	$D(t)$	the CMS service quality evaluation results at the time t
06	$Q(t)$	the CMS equipment security assessment results at the time t
07	$R(t)$	the CMS network security evaluation results at the time t
08	$O(t)$	the CMS network security status evaluation results at the time t

The evaluation indicators involved in equipment safety are the mean time to failure, mean running time, failure repair time, failure frequency and failure severity of equipment. The core of a CMS is service, which aims to provide reliable manufacturing services for users by relying on stable network resources and system components. Therefore, the sudden drop in service quality can reflect the security of the system, so the service quality can also reflect the network security status of the CMS, and the evaluation indicator of service quality is as follows: service integrity, average service response time, service access success rate, and average service time.

According to the security threats faced by the network, the security evaluation indicators are divided into network attack frequency and network attack severity. Fig. 2 shows the architecture of the evaluation metrics proposed in this paper.

B. NETWORK SECURITY STATUS EVALUATION FRAMEWORK OF CMS

1) EVALUATION FRAMEWORK A

According to the evaluation indicator architecture in Fig. 2, this section combines the actual working conditions of the CMS and the reasonable analysis of the importance of cloud security and establishes a three-level evaluation framework A of CMS network security status with the selected important security indicators as the evaluation objects. Considering the threat of cyber attacks to CMS, the addition of the 3rd level indicators to the framework later ensures the rationality of the evaluation framework. Each layer of the framework contains both quantitative data and qualitative knowledge, that is, semiquantitative information. The ER algorithm can fuse semiquantitative information to obtain the NSSA results of the CMS.

In the network security evaluation part, the network attack types of the Edge-IIoTset dataset [28] are divided into Backdoor attack frequency, DDoS attack frequency, Password attack frequency and so on according to the network attack frequency. According to the severity of network attacks, it is divided into Backdoor attack severity, DDoS attack severity, Password attack severity and so on. At the same time, each evaluation indicator is marked with "r", and then the weights of different indicators are calculated according to the entropy weight method, denoted as "ω", to construct the network security status evaluation framework of the CMS, as shown in Table 2.

2) EVALUATION FRAMEWORK B

This section establishes another three-level evaluation framework B for the network security status of the CMS. Different from Framework A, the network security evaluation part takes the attack types in the network part of the TON-IoT dataset [29] as samples and selects representative network attacks to participate in the evaluation of network security. Each attack is evaluated by its attack frequency and attack severity. Evaluation framework B is shown in Table 3.

C. ASSESSMENT LEVELS

This paper refers to the National Internet Emergency Center security indicator classification and uses expert knowledge to divide the fusion results of CMS network security at all levels into five assessment levels, which are as follows: excellent, good, generally dangerous, dangerous and severely dangerous, as shown in Table 4.

This paper also divides each evaluation indicator into five levels, namely, "excellent, good, generally dangerous, dangerous and severely dangerous". At the same time, according to expert experience, the evaluation interval of

TABLE 2. NSSA framework of CMS A.

Indicators	The first grade	The second grade	The third grade
Network Security Status of CMS (r)	Equipment safety (r_1) (ω_1=0.3)	The mean time of equipment failure(r_{11})(ω_{11}=0.1758)	None
		Average operating time of the device (r_{12})(ω_{12}=0.2995)	None
		Device fault repair time (r_{13})(ω_{13}=0.1801)	None
	Equipment safety (r_1) (ω_1=0.3)	Device failure frequency (r_{14})(ω_{14}=0.1657)	None
		The fault severity of the device (r_{15})(ω_{15}=0.1789)	None
	Quality of Service(r_2) (ω_2=0.4)	Average service time(r_{21})(ω_{21}=0.29)	None
		Service access success rate(r_{22})(ω_{22}=0.29)	None
		Integrity of service(r_{23})(ω_{23}=0.2678)	None
		Average service response time (r_{24})(ω_{24}=0.1522)	None
	Network Security(r_3) (ω_3=0.3)	Frequency of network attacks (r_{31})(ω_{31}=0.5)	Backdoor attack frequency(r_{311})(ω_{311}=0.2081)
			DDoS attack frequency(r_{312})(ω_{312}=0.2176)
			Password attack frequency(r_{313})(ω_{313}=0.2132)
			XSS attack frequency(r_{314})(ω_{314}=0.0972)
Network Security Status of CMS (r)	Network Security(r_3) (ω_3=0.3)	Frequency of network attacks (r_{31})(ω_{31}=0.5)	Port_Scanning attack frequency(r_{315})(ω_{315}=0.0628)
			Ransomware attack frequency(r_{316})(ω_{316}=0.1101)
			SQL_injection attack frequency(r_{317})(ω_{317}=0.0725)
			Uploading attack frequency(r_{318})(ω_{318}=0.0185)
		Severity of network attacks (r_{32})(ω_{32}=0.5)	Backdoor attack severity(r_{321})(ω_{321}=0.1658)
			DDoS attack severity(r_{322})(ω_{322}=0.2657)
			Password attack severity(r_{323})(ω_{323}=0.2256)
			XSS attack severity(r_{324})(ω_{324}=0.0255)
			Port_Scanning Severity of attack(r_{325})(ω_{325}=0.0877)
			Ransomware attack severity(r_{326})(ω_{326}=0.0531)
			Ransomware attack severity(r_{326})(ω_{326}=0.0531)
			SQL_injection attack severity(r_{327})(ω_{327}=0.1125)
			Uploading attack severity(r_{328})(ω_{328}=0.0671)

TABLE 3. NSSA framework for CMS B.

Indicators	The first grade	The second grade	The third grade
Network Security Status of CMS (r)	Equipment safety(r_1) (ω_1=0.3)	The mean time of equipment failure(r_{11})(ω_{11}=0.1761)	None
		Average operating time of the device(r_{12})(ω_{12}=0.0437)	None
		Device fault repair time(r_{13})(ω_{13}=0.1297)	None
		Device failure frequency(r_{14})(ω_{14}=0.1762)	None
		The fault severity of the device(r_{15})(ω_{15}=0.4743)	None
	Quality of Service(r_2) (ω_2=0.4)	Average service time(r_{21})(ω_{21}=0.1366)	None
		Service access success rate(r_{22})(ω_{22}=0.1366)	None
		Integrity of service(r_{23})(ω_{23}=0.3089)	None
		Average service response time(r_{24})(ω_{24}=0.4179)	None
	Network Security(r_3) (ω_3=0.3)	DDoS attack(r_{31})(ω_{31}=0.0583)	DDoS attack frequency(r_{311})(ω_{311}=0.5)
			DDoS attack severity(r_{312})(ω_{312}=0.5)
		DoS attack(r_{32})(ω_{32}=0.1609)	DoS attack frequency(r_{321})(ω_{321}=0.5)
			DoS attack severity(r_{322})(ω_{322}=0.5)
		Backdoor attack(r_{33})(ω_{33}=0.4867)	Backdoor attack frequency(r_{331})(ω_{331}=0.5)
			Backdoor attack severity(r_{332})(ω_{332}=0.5)
		Ransomware attack(r_{34})(ω_{34}=0.1131)	Ransomware attack frequency(r_{341})(ω_{341}=0.5)
			Ransomware attack severity(r_{342})(ω_{342}=0.5)
		XSS attack(r_{35})(ω_{35}=0.0729)	XSS attack frequency(r_{351})(ω_{351}=0.5)
			XSS attack severity(r_{352})(ω_{352}=0.5)
		Injection attack(r_{36})(ω_{36}=0.1080)	Injection attack frequency(r_{361})(ω_{361}=0.5)
			Injection attack severity(r_{362})(ω_{362}=0.5)

TABLE 4. CMS network security assessment level.

No.	Evaluation interval	Danger level	Hazard class abbreviation
01	[0-0.4)	excellent	***E***
02	[0.4-0.5)	good	***G***
03	[0.5-0.7)	generally dangerous	***GD***
04	[0.7-0.9)	dangerous	***D***
05	[0.9-1]	severely dangerous	***SD***

quantitative attributes is established to ensure the accuracy of the experimental results.

The evaluation levels of qualitative indicator attributes are also given based on expert experience. The method of using expert knowledge is beneficial to improve the reasoning speed of evidence, reduce the computational complexity, and reflect the real network security status of CMS. The evaluation levels of each security indicator are shown in Table 5.

D. EVALUATION STEPS/ER FUSION DATA PROCESS

According to Table 2 CMS NSSA framework A, the specific assessment steps are given as follows:

Step 1: The ER algorithm is used to fuse the data of the 3rd level indicators, and then the fusion results are classified and fused according to the 2nd level indicators to obtain the evaluation level of the 2nd level security indicators.

Step 2: According to the results of the 2nd level indicators after fusion, the evaluation level of the 1st level three security indicators is obtained.

Step 3: The indicator data of the three dimensions are finally fused to obtain the network security status evaluation level of the CMS. The detailed reasoning process of indicator data fusion is shown in Fig. 3.

To elaborate the detailed process of the ER algorithm to fuse the indicator data, this section takes the network attack frequency evaluation constructed in Table 2 as an example and uses the Edge-IIoTset dataset as the sample data to give the detailed process of the evaluation by using the ER algorithm to fuse the indicator data.

In the set collection of attack types, the unit of attack frequency is times/hour. Taking the data between 2:00 AM and 3:00 AM, backdoor attacks are 0 per hour, DDoS attacks are 0 per hour, password attacks are 0 per hour, XSS attacks are 333 per hour, Port Scanning attacks are 0 per hour, and Ransomware attacks are 0 per hour. The SQL injection attack is 0 times/hour, and the uploading attack is 87 times/hour.

(1) According to formula (1), the confidence of the eight indicator attributes for the five-level evaluation can be obtained $\beta_{i,j}$, $i \in [311, 318], j \in [1, 5]$ as shown in Table 6.

(2) According to the weights given by equations (2) - (5) and Table 2, the above confidence measures can be converted into basic probability mass, that is $P_{i,j}$, $i \in [311, 318], j \in [1, 5]$, and the calculation results are shown in Table 7.

Similarly, when $i \in [311, 318], j = \theta$, calculate $P_{i,j}$, $\overline{P_{i,j}}$ and $Q_{i,j}$, and the results are shown in Table 8.

TABLE 5. Assessment level of each safety index.

Framework	Indicators	*E*	*G*	*GD*	*D*	*SD*
A	r_{11} mins	0.00	5.00	25.00	40.00	60.00
	r_{12} mins	60.00	40.00	20.00	10.00	0.00
	r_{13} mins	0.00	10.00	30.00	40.00	60.00
	r_{14} %	0.00	0.15	0.40	0.70	1.00
	r_{15}	Qualitative indicator				
	r_{21} mins	60.00	40.00	20.00	10.00	0.00
	r_{22} %	100.00	90.00	50.00	30.00	0.00
	r_{23}	Qualitative indicator				
	r_{24} ms	8	100	270	500	729
	r_{311} times/h	0	230	550	2100	4965
	r_{312} times/h	0	280	820	1580	2020
	r_{313} times/h	0	470	1970	2240	2460
	r_{314} times/h	0	360	400	450	788
	r_{315} times/h	0	440	600	720	1202
	r_{316} times/h	0	700	960	2010	4957
	r_{317} times/h	0	580	680	830	2058
	r_{318} times/h	0	90	430	920	2548
	r_{321}	Qualitative indicator				
	r_{322}	Qualitative indicator				
	r_{323}	Qualitative indicator				
	r_{324}	Qualitative indicator				
	r_{325}	Qualitative indicator				
	r_{326}	Qualitative indicator				
	r_{327}	Qualitative indicator				
B	r_{11} mins	0.00	5.00	25.00	40.00	60.00
	r_{12} mins	60.00	40.00	20.00	10.00	0.00
	r_{13} mins	0.00	10.00	30.00	40.00	60.00
	r_{14} %	0.00	0.15	0.40	0.70	1.00
	r_{15}	Qualitative indicator				
	r_{21} mins	60.00	50.00	40.00	30.00	20.00
	r_{22} %	0.99	0.90	0.75	0.55	0.35
	r_{23}	Qualitative indicator				
	r_{24} ms	0	50	100	200	255
	r_{311} times/h	0	100	200	300	700
	r_{312}	Qualitative indicator				
	r_{321} times/h	0	200	300	400	500
	r_{322}	Qualitative indicator				
	r_{331} times/h	0	100	200	300	500
	r_{332}	Qualitative indicator				
	r_{341} times/h	0	50	100	200	300
	r_{342}	Qualitative indicator				
	r_{351} times/h	0	100	200	500	1000
	r_{352}	Qualitative indicator				
	r_{361} times/h	0	200	500	1000	1500
	r_{362}	Qualitative indicator				

(3) Calculate the scale factor $K_{I(i+1)} = K_{I(312)}$.

$$K_{I(312)} = \frac{1}{1 - \sum_{k=1}^{N} \sum_{\substack{j=1 \\ j \neq k}}^{N} P_{I(312),k} P_{311,j}} = \frac{1}{1-0} = 1$$

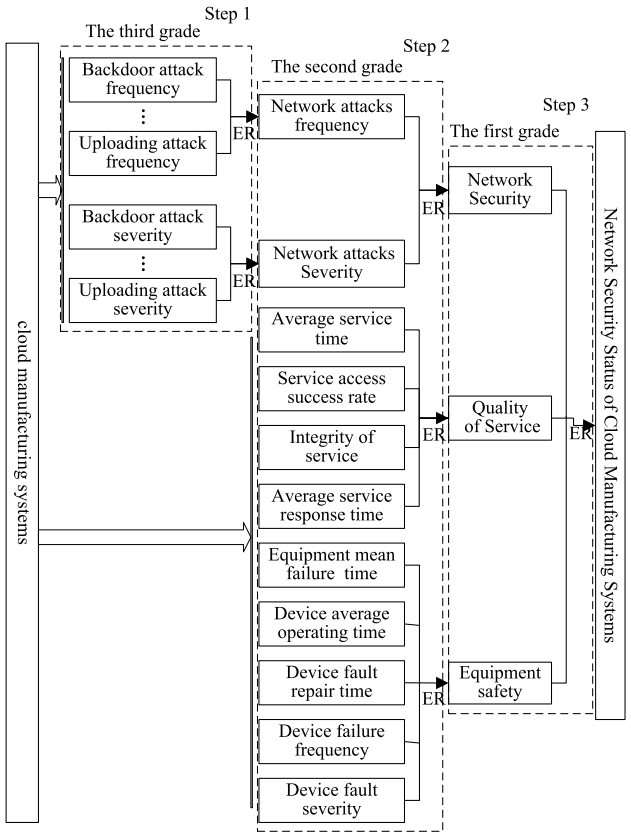


FIGURE 3. ER fusion indicator data inference process.

TABLE 6. The belief degrees.

i	j				
	1	2	3	4	5
311	1.0000	0.0000	0.0000	0.0000	0.0000
312	1.0000	0.0000	0.0000	0.0000	0.0000
313	1.0000	0.0000	0.0000	0.0000	0.0000
314	0.0750	0.9250	0.0000	0.0000	0.0000
315	1.0000	0.0000	0.0000	0.0000	0.0000
316	1.0000	0.0000	0.0000	0.0000	0.0000
317	1.0000	0.0000	0.0000	0.0000	0.0000
318	0.0333	0.9667	0.0000	0.0000	0.0000

TABLE 7. The basic probability mass.

i	j				
	1	2	3	4	5
311	0.2081	0.0000	0.0000	0.0000	0.0000
312	0.2176	0.0000	0.0000	0.0000	0.0000
313	0.2132	0.0000	0.0000	0.0000	0.0000
314	0.0073	0.0899	0.0000	0.0000	0.0000
315	0.0628	0.0000	0.0000	0.0000	0.0000
316	0.1101	0.0000	0.0000	0.0000	0.0000
317	0.0725	0.0000	0.0000	0.0000	0.0000
318	0.0006	0.0179	0.0000	0.0000	0.0000

(4) The probability mass of fused $I(312)$ can be calculated according to formulas (6)∼(9).

$$
\begin{aligned}
P_{I(312),1} &= K_{I(312)}[P_{I(311),1}P_{312,1} + P_{I(311),1}P_{312,\theta} \\
&\quad + P_{I(311),\theta}P_{312,1}] \\
&= 1 \times [0.2081 \times 0.2176 + 0.2081 \times 0.7824 \\
&\quad + 0.7919 \times 0.2176] \\
&= 0.3804 \\
P_{I(312),2} &= K_{I(312)}[P_{I(311),2}P_{312,2} + P_{I(311),2}P_{312,\theta} \\
&\quad + P_{I(311),\theta}P_{312,2}] \\
&= 1 \times [0 \times 0 + 0 \times 0.7824 + 0.7919 \times 0] = 0 \\
P_{I(312),3} &= K_{I(312)}[P_{I(311),3}P_{312,3} + P_{I(311),3}P_{312,\theta} \\
&\quad + P_{I(311),\theta}P_{312,3}] \\
&= 1 \times [0 \times 0 + 0 \times 0.7824 + 0.7919 \times 0] = 0 \\
P_{I(312),4} &= K_{I(312)}[P_{I(311),4}P_{312,4} + P_{I(311),4}P_{312,\theta} \\
&\quad + P_{I(311),\theta}P_{312,4}] \\
&= 1 \times [0 \times 0 + 0 \times 0.7824 + 0.7919 \times 0] = 0 \\
P_{I(312),5} &= K_{I(312)}[P_{I(311),5}P_{312,5} + P_{I(311),5}P_{312,\theta} \\
&\quad + P_{I(311),\theta}P_{312,5}] \\
&= 1 \times [0 \times 0 + 0 \times 0.7824 + 0.7919 \times 0] = 0 \\
Q_{I(312),\theta} &= K_{I(312)}[Q_{I(311),\theta}Q_{312,\theta} + Q_{I(311),\theta}\overline{P_{312,\theta}} \\
&\quad + \overline{P_{I(311),\theta}}Q_{312,\theta}] \\
&= 1 \times [0 \times 0 + 0 \times 0.7824 + 0.7919 \times 0] = 0 \\
\overline{P_{I(312),\theta}} &= K_{I(312)}[\overline{P_{I(311),\theta}P_{312,\theta}}] \\
&= 1 \times 0.7919 \times 0.7824 = 0.6196 \\
P_{I(312),\theta} &= \overline{P_{I(312),\theta}} + Q_{I(312),\theta} = 0.6196
\end{aligned}
$$

TABLE 8. The basic probability mass.

i	$P_{i,j}$	$\overline{P_{i,j}}$	$Q_{i,j}$
311	0.7919	0.7919	0.0000
312	0.7824	0.7824	0.0000
313	0.7868	0.7868	0.0000
314	0.9028	0.9028	0.0000
315	0.9372	0.9372	0.0000
316	0.8899	0.8899	0.0000
317	0.9725	0.9275	0.0000
318	0.9815	0.9815	0.0000

(5) Similarly, the probability mass of scale factor $K_{I(313)}$, $K_{I(314)}$, $K_{I(315)}$, $K_{I(316)}$, $K_{I(317)}$, $K_{I(318)}$ and $I(313)$, $I(314)$, $I(315)$, $I(316)$, $I(317)$, $I(318)$ can be calculated, the calculation process is omitted, and the results are shown in Table 9.

(6) The confidence degree of the network attack frequency (r_{31}) obtained by the fusion of the eight-level indicators can be obtained by formulas (11) and (12) as follows:

$$
\begin{aligned}
\sigma_1 &= \frac{P_{I(318),1}}{1 - \overline{P_{I(318),\theta}}} = \frac{0.5994}{1 - 0.3579} = 0.9335 \\
\sigma_2 &= \frac{P_{I(318),2}}{1 - \overline{P_{I(318),\theta}}} = \frac{0.0427}{1 - 0.3579} = 0.0665 \\
\sigma_3 &= \frac{P_{I(318),3}}{1 - \overline{P_{I(318),\theta}}} = \frac{0}{1 - 0.3579} = 0 \\
\sigma_4 &= \frac{P_{I(318),4}}{1 - \overline{P_{I(318),\theta}}} = \frac{0}{1 - 0.3579} = 0
\end{aligned}
$$

TABLE 9. Scale factor and probability mass.

i	$K_{I(i)}$	$P_{I(i),1}$	$P_{I(i),2}$	$P_{I(i),3}$	$P_{I(i),4}$	$P_{I(i),5}$	$Q_{I(i),\theta}$	$\overline{P_{I(i),\theta}}$	$P_{I(i),\theta}$
313	1.0000	0.5125	0.0000	0.0000	0.0000	0.0000	0.0000	0.4875	0.4875
314	1.0483	0.4927	0.0459	0.0000	0.0000	0.0000	0.0000	0.4614	0.4614
315	1.0029	0.5232	0.0431	0.0000	0.0000	0.0000	0.0000	0.4337	0.4337
316	1.0048	0.5737	0.0385	0.0000	0.0000	0.0000	0.0000	0.3878	0.3878
317	1.0028	0.6035	0.0358	0.0000	0.0000	0.0000	0.0000	0.3607	0.3607
318	1.0109	0.5994	0.0427	0.0000	0.0000	0.0000	0.0000	0.3579	0.3579

TABLE 10. Evaluation results (%).

No.	Assessment Levels	*E*	*G*	*GD*	*D*	*SD*
01	r_{32}	92.48	7.52	0.00	0.00	0.00
02	r_3	99.44	0.56	0.00	0.00	0.00
03	r_2	9.50	0.00	0.00	0.00	90.50
04	r_1	73.07	0.00	0.00	0.00	26.93
05	r	60.23	0.62	0.00	0.00	39.15

$$\sigma_5 = \frac{P_{I(318),5}}{1-\overline{P_{I(318),\theta}}} = \frac{0}{1-0.3579} = 0$$
$$\sigma_\theta = \frac{Q_{I(318),\theta}}{1-\overline{P_{I(318),\theta}}} = \frac{0}{1-0.3579} = 0$$

Through the above calculation, it can be concluded that the security state evaluation results determined by the network attack frequency (r_{31}) are {excellent (93.35%), good (6.65%), generally dangerous (0%), dangerous (0%), and severely dangerous (0%)}. Indicates an evaluation rating of "excellent" for the frequency of attacks between 2:00 AM and 3:00 AM. The correctness of the calculated results is verified by simulation experiments in Section V.

V. SIMULATION EXPERIMENT

A. EXPERIMENTAL RESULTS AND ANALYSIS

The calculation process in Section IV-D is the detailed process of using the ER algorithm to fuse the indicator data. The fusion steps of other indicator data are the same as the calculation process in Section IV-D. Due to space limitations, this paper will not elaborate on each one but only gives the evaluation results between 2:00 AM and 3:00 AM. The specific evaluation results of network attack severity (r_{32}), network security (r_3), service quality (r_2), network equipment security (r_1) and network security status (r) of the CMS are shown in Table 10.

Table 10 shows that the evaluation grade of network attack severity between 2:00 AM and 3:00 AM is "***E***"; network security is assessed as "***E***"; the evaluation level of service quality is "***SD***"; the evaluation level of network equipment security is "***E***"; and the network security status evaluation level of the CMS is "***E***".

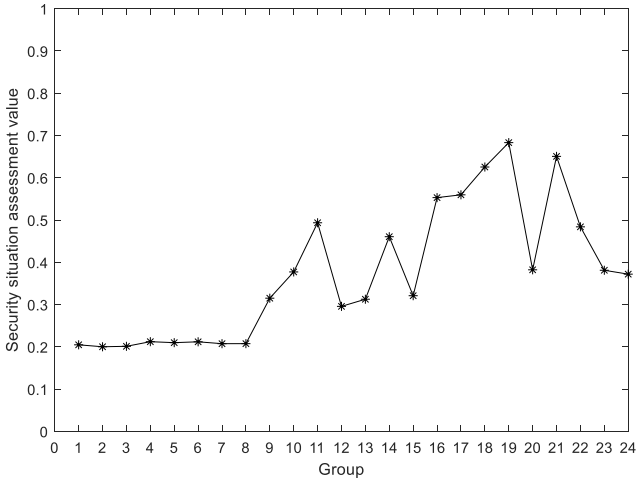


FIGURE 4. Network attack frequency evaluation results.

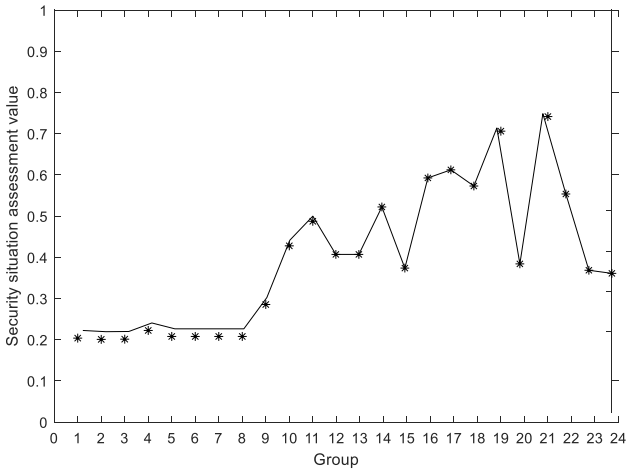


FIGURE 5. Evaluation results of the severity of network attacks.

1) SIMULATION EXPERIMENT 1

The Edge-IIoTset dataset was selected to complete the evaluation of network attack frequency and network attack severity. The dataset was sorted, screened and counted, and the data from 24 hours were selected for ER fusion. The evaluation results are shown in Fig. 4 and Fig. 5.

Fig. 4 and Fig. 5 show that the security state evaluation value between 2:00 AM and 3:00 AM is 0.2. It indicates that there are few network attacks during this period, all devices are running normally, and the system is in a relatively secure state. According to the evaluation level divided in Section IV-C, the security status determined by network attack frequency and network attack severity can be evaluated as "***E***", which is in line with the example calculation results in Section IV-D and the evaluation results of r_{32} in Table 10.

The ER algorithm is used to fuse the security situation assessment values of network attack frequency and network attack severity, and the network security assessment results are obtained. In the two parts of service quality evaluation and network equipment security evaluation, the quantitative information was randomly generated according to the actual situation of the CMS, and the qualitative indicators are

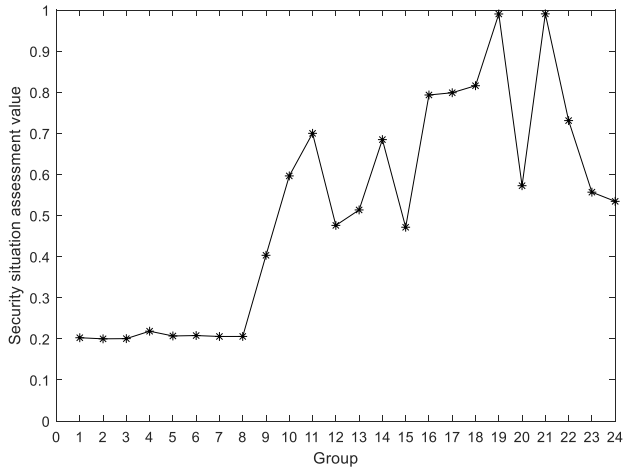


FIGURE 6. Network security assessment results.

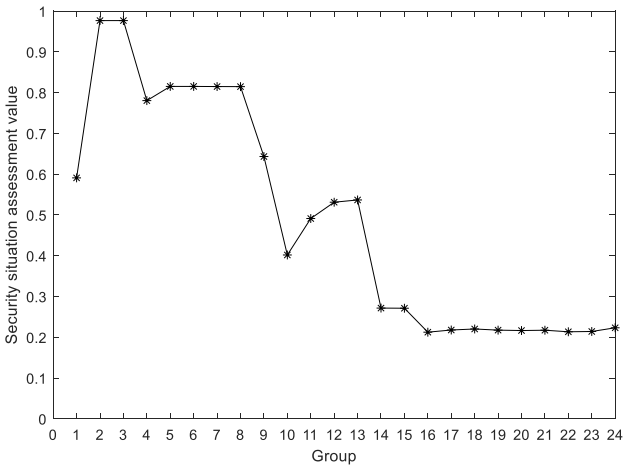


FIGURE 7. Service quality assessment results.

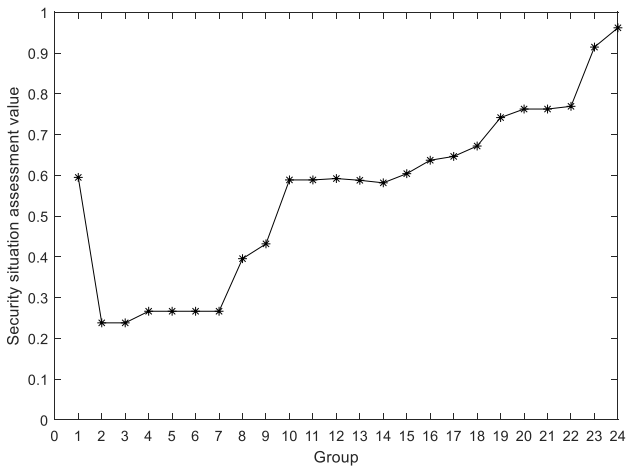


FIGURE 8. Network equipment security assessment results.

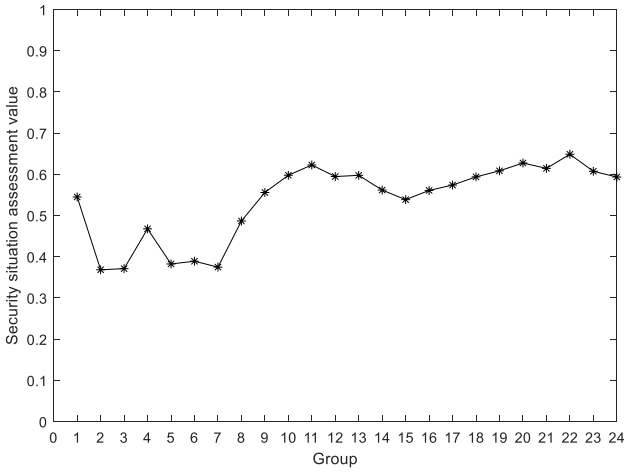


FIGURE 9. The NSSA results of CMS.

specified according to expert knowledge. The results of the network security evaluation, quality of service evaluation and network equipment security evaluation are shown in Figs. 6, 7 and 8, respectively.

Fig. 6 shows that between 2:00 AM and 3:00 AM, the security situation assessment value is between 0.2 and 0.3. This indicates that the network attacks on the system during this period are weak, the device is in normal running state, and the system as a whole is in a relatively secure state. According to the assessment level divided in Section IV-C, the state determined by network security can be evaluated as "***E***", which is in line with the assessment results of r_3 in Table 10.

Fig. 6 shows that at approximately 19:00 and 21:00 at night, the security situation assessment value is close to 1, indicating that the system is under serious attack and the equipment may not operate normally, which is judged as "***SD***".

Similarly, Fig. 7 and Fig. 8 show that in the same time, the security situation assessment value of service quality is greater than 0.9 and less than 1, and it is evaluated as "***SD***"; the security situation assessment value of network equipment is approximately 0.25, and it is evaluated as "***E***". All results agree with the evaluation results of r_2 and r_1 in Table 10.

The ER algorithm is used to fuse the assessment results of network equipment security, service quality and network security, and the ER algorithm is used to fuse the security situation assessment values of the above three parts again to obtain the final NSSA results of the CMS. The evaluation results are shown in Fig. 9.

Fig. 9 shows that the security situation assessment value between 2:00 AM and 3:00 AM is approximately 0.35. According to the evaluation level constructed in Section IV-C, the CMS network status is evaluated as "***E***", which is in line with the assessment result of r in Table 10. At 11:00 AM, the point CMS network security status is the worst, rated as dangerous. That is, the smaller the value is, the closer to the X-axis, and the better the network security status of the CMS.

2) SIMULATION EXPERIMENT 2

The network part of the TON-IoT dataset was selected to complete the evaluation of the network security part. The dataset was sorted, screened and counted, and a total of 96 data points in 4 days were selected for ER fusion. The

TABLE 11. Evaluation value and results of the CMS network security status of each algorithm.

No.	ER		SVM		BP		RF		KNN	
	Evaluation Value	Evaluation Results	Evaluation Value	Evaluation Results	Evaluation Value	Evaluation Results	Evaluation Value	Evaluation Results	Evaluation Value	Evaluation Results
01	0.4035	*G*	0.4312	*G*	0.2706	*E*	0.4312	*G*	0.4312	*G*
02	0.3376	*E*	0.4866	*G*	0.4682	*G*	0.3453	*E*	0.4866	*G*
03	0.4897	*G*	0.4812	*G*	0.4798	*G*	0.4812	*G*	0.4812	*G*
04	0.4983	*G*	0.4812	*G*	0.4883	*G*	0.4919	*G*	0.4812	*G*
05	0.4895	*G*	0.4866	*G*	0.5033	*GD*	0.3900	*E*	0.4866	*G*
06	0.5017	*GD*	0.4812	*G*	0.4974	*G*	0.4765	*G*	0.4812	*G*
07	0.5094	*GD*	0.4812	*G*	0.4820	*G*	0.5829	*GD*	0.4812	*G*
08	0.4863	*G*	0.4765	*G*	0.4887	*G*	0.4700	*G*	0.4700	*G*
09	0.5359	*GD*	0.5462	*GD*	0.5434	*GD*	0.4694	*G*	0.5462	*GD*
10	0.5341	*GD*	0.5517	*GD*	0.5446	*GD*	0.5416	*GD*	0.5462	*GD*
11	0.5142	*GD*	0.5153	*GD*	0.5241	*GD*	0.5358	*GD*	0.5153	*GD*
12	0.5321	*GD*	0.5358	*GD*	0.5495	*GD*	0.5484	*GD*	0.5354	*GD*
13	0.5400	*GD*	0.5358	*GD*	0.5355	*GD*	0.5373	*GD*	0.5358	*GD*
14	0.5231	*GD*	0.5358	*GD*	0.5623	*GD*	0.4700	*G*	0.4997	*G*
15	0.4742	*G*	0.4421	*G*	0.5249	*GD*	0.5462	*GD*	0.4421	*G*
16	0.4745	*G*	0.4257	*G*	0.3491	*E*	0.8419	*D*	0.8419	*D*
17	0.4561	*G*	0.4421	*G*	0.4725	*G*	0.5358	*GD*	0.4421	*G*
18	0.4613	*G*	0.4845	*G*	0.4559	*G*	0.5484	*GD*	0.4845	*G*
19	0.5171	*GD*	0.4765	*G*	0.4994	*G*	0.4919	*G*	0.4765	*G*
20	0.5816	*GD*	0.4812	*G*	0.5042	*GD*	0.5327	*GD*	0.4812	*G*
21	0.4844	*G*	0.4866	*G*	0.4885	*G*	0.3900	*E*	0.4866	*G*
22	0.5284	*GD*	0.4421	*G*	0.4246	*G*	0.3453	*E*	0.4312	*G*
23	0.4366	*G*	0.4421	*G*	0.3052	*E*	0.4812	*G*	0.4312	*G*
24	0.3734	*E*	0.4997	*G*	0.4903	*G*	0.3684	*E*	0.3684	*E*

Note: *E* for excellent, *G* for good, *GD* for generally dangerous, *D* for dangerous, and *SD* for severely dangerous.

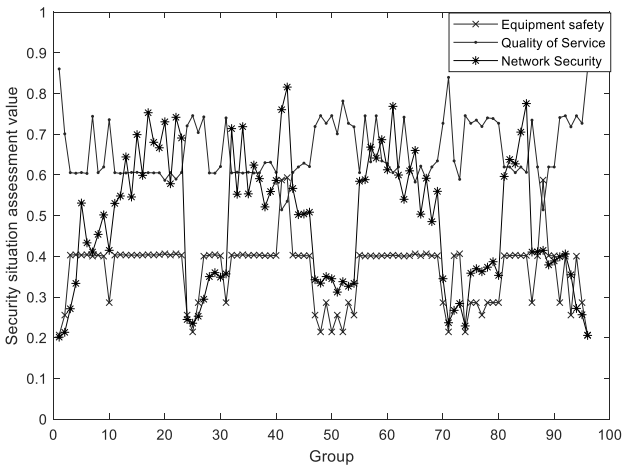


FIGURE 10. Network device, service quality, and network security evaluation results.

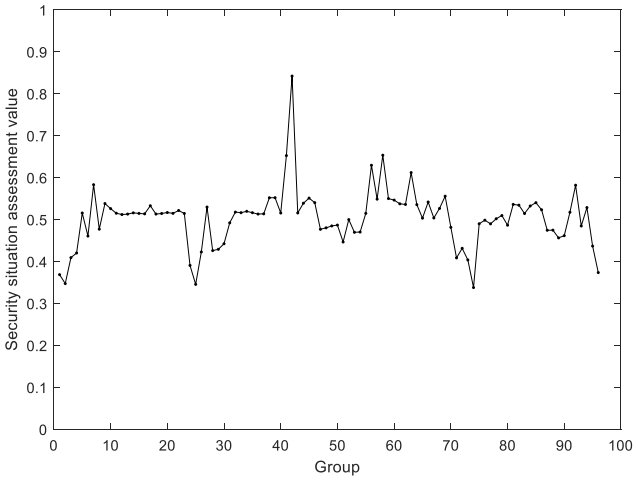


FIGURE 11. The NSSA results of CMS.

data of network equipment security evaluation and service quality evaluation were randomly generated according to the attack frequency and attack severity. The evaluation results are shown in Fig. 10.

Similarly, the final NSSA results of the CMS can be obtained by fusing the security situation assessment values of the three parts. This is shown in Fig. 11.

The analysis of Fig. 11 shows that the security situation assessment value is the largest around Group 43, indicating that the CMS receives very serious network attacks during this period, and the network security status of the CMS can be evaluated as "***D***".

B. COMPARATIVE EXPERIMENT AND ANALYSIS

In this section, common machine learning methods were used to carry out comparative experiments. Seventy-two data points over three days were selected as the training set, and 24 data points over one day were selected as the test set, which was used to communicate with the support vector

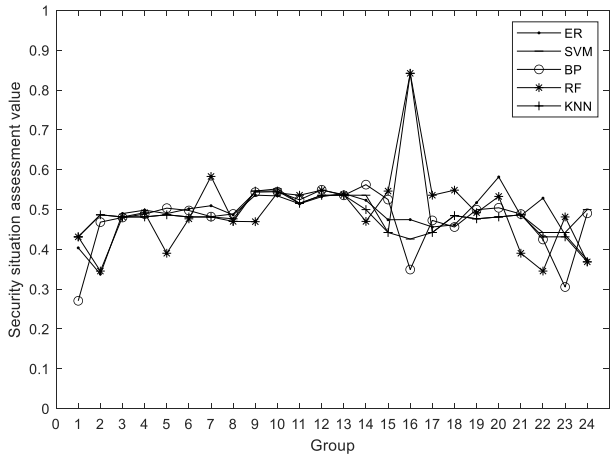


FIGURE 12. Evaluation results of CMS network security status under different algorithms.

machine (SVM) and back propagation (BP). The random forest (RF) algorithm was compared with the K-nearest neighbor (KNN) algorithm. The evaluation value obtained by each algorithm is shown in Fig. 12.

By analyzing Fig. 12, the overall change trend of the NSSA value of the CMS of each model is roughly similar. However, the evaluation value obtained by the ER algorithm is more in line with the actual evaluation value and fits the actual situation, because it can make comprehensive use of semi-quantitative information, effectively use the qualitative information such as expert knowledge, and deal with the uncertain information in the evaluation process. However, machine learning algorithms can only evaluate the network security state of cloud manufacturing systems based on quantitative information, and cannot effectively use qualitative knowledge. The evaluation values and results of the network security status of the CMS for each algorithm are shown in Table 11.

Table 11 shows that the RF and KNN algorithms have large evaluation values from 15:00 to 16:00, which is "***D***"; SVM and BP have small evaluation values from 5:00 to 7:00, which is "***G***"; SVM, BP and KNN have multiple low evaluation values from 19:00 to 23:00, etc. These results have large errors with the actual results. This may not be more accurate to obtain the network security status of the CMS.

In conclusion, compared with the RF, BP, SVM and KNN models, the industrial control heterogeneous network security assessment method based on semiquantitative information has higher assessment accuracy and can more accurately evaluate the network security status of CMS.

VI. CONCLUSION

At present, in the field of network security assessment, there is a lack of methods to reasonably assess the network security status of complex CMSs. Therefore, a method of NSSA of CMS based on semiquantitative information is proposed in this paper. First, through in-depth analysis of the mechanism of CMS network security indicators, reasonable indicators are selected, the weights of each evaluation indicator are calculated, and a CMS network security status evaluation framework including three-level indicators is built. Second, the ER algorithm is used to select the field management layer and the field equipment layer to evaluate the network security status of the CMS, and various uncertain information, including quantitative data and qualitative knowledge, is fused. An example is given to illustrate the detailed steps of the integration of indicator data by the ER algorithm. Third, the evaluation results of the network security status of the CMS are obtained by using ER fusion of the evaluation results of the 1st level security indicators, and the security level is determined. Finally, through experimental verification, the proposed method is more accurate and can obtain more realistic evaluation results. In future studies, the evaluation method should be further optimized to improve the accuracy.

The ER-based network security state assessment method of CMS proposed in this paper has potential engineering application value and can provide an effective way to solve the network security assessment problem of complex dynamic systems. However, this method also has limitations. First, in practice, the reliability of data acquired by sensors cannot be guaranteed due to the existence of uncertainties, which will affect the rationality of the evaluation results. Second, if the experts are inexperienced, the accuracy of the evaluation results will be affected. Finally, the environment of CMS is very complex, and it will inevitably be interfered by real environmental noise and external environmental factors, which will also affect the accuracy of security state acquisition. Therefore, in future studies, it is necessary to further consider the reliability of sensor data when using the ER method for data fusion, and further optimize the proposed method to improve the accuracy of the evaluation results.

REFERENCES

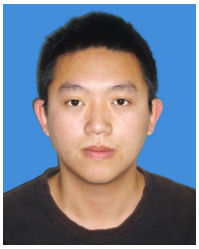
[1] G. Adamson, L. Wang, M. Holm, and P. Moore, "Cloud manufacturing—A critical review of recent development and future trends," *Int. J. Comput. Integr. Manuf.*, vol. 30, nos. 4–5, pp. 347–380, Apr. 2015.
[2] B. H. Li, "Cloud manufacturing system 3.0—A new intelligent manufacturing system in the era of 'intelligence+,'" *Comput. Integr. Manufaturing Syst.*, vol. 25, no. 12, pp. 2997–3012, Dec. 2019.
[3] A. Corallo, M. Lazoi, M. Lezzi, and P. Pontrandolfo, "Cybersecurity challenges for manufacturing systems 4.0: Assessment of the business impact level," *IEEE Trans. Eng. Manag.*, early access, Jun. 16, 2022, doi: 10.1109/TEM.2021.3084687.
[4] V. Mullet, P. Sondi, and E. Ramat, "A review of cybersecurity guidelines for manufacturing factories in industry 4.0," *IEEE Access*, vol. 9, pp. 23235–23263, 2021.
[5] N. Kaloudi and J. Li, "The AI-based cyber threat landscape: A survey," *ACM Comput. Surv.*, vol. 53, no. 1, pp. 1–34, Feb. 2020.
[6] O. Aslan and R. Samet, "A comprehensive review on malware detection approaches," *IEEE Access*, vol. 8, pp. 6249–6271, 2020.
[7] L. He, T. Wan, C. Zhang, F. Xia, S. Wang, and Y. Wang, "Network situation assessment of host node based on improved D-S evidence theory," *J. Phys., Conf. Ser.*, vol. 1738, no. 1, Jan. 2021, Art. no. 012091.
[8] R. Henzel and G. Herzwurm, "Cloud manufacturing: A state-of-the-art survey of current issues," *Proc. CIRP*, vol. 72, pp. 947–952, Jul. 2018.
[9] G. Ma, Y. G. Du, X. Yang, B. Zhang, and Z. Z. Shi, "Expert system for risk assessment of complex systems," *J. Tsinghua Univ. Natural Sci. Ed.*, vol. 56, no. 1, pp. 66–76, Jan. 2016.
[10] P. Munk and A. Nordmann, "Model-based safety assessment with SysML and component fault trees: Application and lessons learned," *Softw. Syst. Model.*, vol. 19, no. 4, pp. 889–910, Feb. 2020.

[11] Z. Y. Chen and M. W. L., "Hesitant fuzzy language envelope analysis model based on analytic hierarchy process and its application in network security evaluation of edge nodes," *Comput. Appl. Res.*, vol. 38, no. 1, pp. 209–214, Apr. 2021.
[12] X. Q. Li, Y. Liu, and S. Y. Bao, "Application of D-S evidence theory in missile health assessment," *Meas. Control Technol.*, vol. 41, no. 3, pp. 26–32, Sep. 2022.
[13] X. Li and Y. Duan, "Network security situation assessment method based on improved hidden Markov model," *Comput. Sci.*, vol. 47, no. 7, pp. 287–291, 2020.
[14] J. Yuan, F. L. Wang, S. Wang, and L. P. Zhao, "Fault diagnosis method of hybrid expert knowledge system based on D-S fusion," *J. Automat.*, vol. 43, no. 9, pp. 1580–1587, Aug. 2017.
[15] M. Khosravi-Farmad and A. Ghaemi-Bafghi, "Bayesian decision network-based security risk management framework," *J. Netw. Syst. Manage.*, vol. 28, no. 4, pp. 1794–1819, Aug. 2020.
[16] M. Wu, Z. Song, and Y. B. Moon, "Detecting cyber-physical attacks in CyberManufacturing systems with machine learning methods," *J. Intell. Manuf.*, vol. 30, no. 3, pp. 1111–1123, Mar. 2019.
[17] S. C. Ye, "Research on model-based network security risk assessment method," *Inf. Comput. Theory Ed.*, vol. 34, no. 7, pp. 138–142, Apr. 2022.
[18] X. Qiu, Y. Dai, Y. Xiang, and L. Xing, "A hierarchical correlation model for evaluating reliability, performance, and power consumption of a cloud service," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 46, no. 3, pp. 401–412, Mar. 2016.
[19] A. Aldweesh, A. Derhab, and A. Z. Emam, "Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues," *Knowl.-Based Syst.*, vol. 189, Feb. 2019, Art. no. 105124.
[20] Z.-J. Zhou, C.-H. Hu, G.-Y. Hu, X.-X. Han, B.-C. Zhang, and Y.-W. Chen, "Hidden behavior prediction of complex systems under testing influence based on semiquantitative information and belief rule base," *IEEE Trans. Fuzzy Syst.*, vol. 23, no. 6, pp. 2371–2386, Dec. 2015.
[21] F. J. Zhao, Z. J. Zhou, C. H. Hu, L. L. Chang, and L. Wang, "On line evaluation method of dynamic system security based on evidential reasoning," *J. Automat.*, vol. 43, no. 11, pp. 1950–1961, 2017.
[22] S. T. Liu, X. J. Li, Z. J. Zhou, J. P. Yao, and J. Wang, "Overview of the application of evidence theory in pattern classification," *J. Chin. Acad. Electron. Sci.*, vol. 17, no. 3, pp. 247–258, Mar. 2022.
[23] Z. J. Zhou, T. Y. Liu, G. Y. Hu, S. Z. Li, G. L. Li, and W. He, "A fault detection method based on data reliability and interval evidential reasoning," *J. Automat.*, vol. 46, no. 12, pp. 2628–2637, 2020.
[24] G. Q. Qiu and Y. F. Gu, "Fault detection of relay contact system based on interval evidential reasoning," *J. Electron. Meas. Instrum.*, vol. 36, no. 6, pp. 126–133, Jun. 2022.
[25] W. Bi, F. Gao, and A. Zhang, "A novel weapon system effectiveness assessment method based on the interval-valued evidential reasoning algorithm and the analytical hierarchy process," *IEEE Access*, vol. 9, pp. 53480–53490, 2021.
[26] J. Wang, Z.-J. Zhou, C.-H. Hu, S.-W. Tang, and Y. Cao, "A new evidential reasoning rule with continuous probability distribution of reliability," *IEEE Trans. Cybern.*, vol. 52, no. 8, pp. 8088–8100, Aug. 2022.
[27] H. Wei and P. L. Qiao, "Reliability assessment of cloud computing platform based on semiquantitative information and evidential reasoning," *J. Control Sci. Eng.*, vol. 2016, Nov. 2016, Art. no. 2670210.
[28] M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, and H. Janicke, "Edge-IIoTset: A new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning," *IEEE Access*, vol. 10, pp. 40281–40306, 2022.
[29] A. Alsaedi, N. Moustafa, Z. Tari, A. Mahmood, and A. Anwar, "TON_IoT telemetry dataset: A new generation dataset of IoT and IIoT for data-driven intrusion detection systems," *IEEE Access*, vol. 8, pp. 165130–165150, 2020.

SHIMING LI received the M.D. degree from the Harbin Institute of Technology. He is currently an Associate Professor with the College of Computer Science and Information Engineering, Harbin Normal University (HRBNU), China Computer Society (CCF 37474M). His main research interests include network and information security, industrial internet, and the Internet of Things.

XINGSHUO XU was born in China, in 2000. He is currently pursuing the master's degree with Harbin Normal University. His research interests include network and information security.

GUOHUI ZHOU received the Ph.D. degree from the Changchun Institute of Optics, Fine Mechanics and Physics, Chinese Academy of Sciences, Changchun, China. He has published more than 20 articles in journals. His current research interests include artificial intelligence, pattern recognition, and embedded systems. He received the Second Prize of the Scientific and Technological Progress of Heilongjiang Province.



YUHE WANG received the B.Eng. and Ph.D. degrees from the Harbin University of Science and Technology, Harbin, Heilongjiang, China, in 2012 and 2019, respectively. He was a Lecturer with the Changchun University of Technology. He is currently a Lecturer with Harbin Normal University, Harbin. He has published approximately five articles. His research interests include intelligent computing, industrial network security, and belief rule base.

ZHICONG LI received the M.D. degree from the Harbin Institute of Technology. He is currently an Associate Professor with the College of Computer Science and Information Engineering, Harbin Normal University (HRBNU). His research interests include three-branch decision making and data analysis.

YAN ZHAO received the Ph.D. degree from the College of Network and Space Security, PLA Information Engineering University, in 2019. She is currently with the School of Information Technology, Luoyang Normal University. Her research interests include information security, the Internet of Things, and embedded systems.

WEIQI ZHAO was born in 2003. She is currently pursuing the bachelor's degree in computer science and technology with Jilin University. Her research interests include network security and deep learning.