An Integrated Assessment Scheme of Network Infrastructure Following Security Standards and Specifications

Zhaoyang Li[1,2], Hao Duan[1,3], Jiarui Lei[1,3], Zijiang Yang[4], Feng Lin[4], Yumei Li[4], and Zhiwei Zhang[1,5,*]
[1]School of Computer Science and Technology, Xidian University, Xi’an, Shaanxi, 710071, China
[2]Qingdao Institute of Computing Technology, Xidian University, Qingdao, Shandong, 266109, China
[3]Guangzhou Institute of Technology, Xidian University, Guangzhou, Guangdong, 510555, China
[4]ZhongXinDa Information Technology Co., Ltd., Haikou, Hainan, 570100, China
[5]Hebei Key Laboratory of Network and Information Security, Hebei Normal University, Shijiazhuang, Hebei, 050024, China
[*]Corresponding author

In this intelligent era, with deeper research, faster development, and wider application of information technologies, the network infrastructure plays one more and more important role in data communication and processing that affects almost every field worldwide. Correspondingly, cyberspace security, especially the security of network infrastructure has become elementary for countries and companies. Then, various security standards and specifications have been proposed to guide network infrastructure’s design, development, and operation. Consequently, it is the key to assess whether a network infrastructure is compliant with the related standards and specifications. However, most of the existing security assessment schemes are manual, that is, testers should check all issues depending on their understanding of the network infrastructures and related documents. That results in the lack of accuracy, continuity as well as comprehensiveness. Therefore, in this paper, we propose an AI-based network infrastructure security assessment (ISA-CN) scheme, which concerns China’s current fundamental network infrastructure security assessment related standards and specifications and evaluates the object’s security states with multi-dimensional automatically monitored network traffic data continuously and comprehensively. The analytical and experimental results show that our ISA-CN scheme is suitable for the assessment of real-world network infrastructure systems.

***Index Terms*—Deep Belief Network, Intrusion Detection, Hierarchical Evaluation Model, National Standard, Network Infrastructure**

I. Introduction

In this intelligent era, with deeper research of information technologies, the network infrastructure plays important role in data communication and processing that affects almost every field worldwide such as global economy, military, and politics. Correspondingly, cyberspace security, especially the security of network infrastructure has become elementary for countries and companies. The security protection of information infrastructure has become an important guarantee for countries to promote the development of the digital economy and participate in international competition. Then, various security standards and specifications have been proposed to guide network infrastructure’s design, development, and operation.

In 2014 the United States released the “Improving Critical Infrastructure Cybersecurity”[1]. The framework defines a set of risk management and control processes that apply to critical infrastructure security. For critical information infrastructure, the Ministry of Security has developed a network security capability maturity model to guide operators to conduct security assessments on their systems and other information assets. Organizational security capabilities are assessed. In the same year, the European Network and Information Security Agency (ENISA) published the “Methodologies for the identification of Critical Information Infrastructure assets and services”, which provides methods for identifying services and assets in critical information infrastructure[2]. Subsequently, technical guidance documents such as “Stocktaking, Analysis and Recommendations on the protection of CIIs”[3] and “Technical Guidelines for the implementation of minimum security measures for Digital Service Providers”[4] have been published. The document provides standardized recommendations for public-private cooperation, security incident drills, risk assessment, information sharing, and establishment of controls in critical information infrastructure.

Based on the security features of critical infrastructure, China has systematically carried out standard formulation and standard pilot work from the dimensions of data security, information sharing, monitoring, and early warning, aiming to strengthen the security of critical infrastructure.

While various security standards and specifications have been proposed to guide the design, development, and operation of network infrastructure. Among the existing assessment schemes, there are mainly based on vulnerabilities or current system asset usage. In the vulnerability-based scheme [5], the sub-tasks include the establishment of a vulnerability database, system vulnerability scanning, and a final vulnerability-based security assessment algorithm. This kind of evaluation scheme can better analyze the vulnerability utilization for the existing vulnerabilities, but it cannot effectively evaluate zero-day attacks. This is because the subsequent update of the vulnerability database relies on the manual search of the third-party expert knowledge base by security analysts. However, after finding the latest vulnerability database, it is necessary to manually write matching rules to adapt to the output format

Manuscript received February 25, 2022; revised August 10, 2022. Corresponding author: Zhiwei Zhang (email:zwzhang@xidian.edu.cn).

of the current vulnerability scan, which leads to security problems. It takes analysts several days to check whether the updated system can operate normally because the current algorithm for exploiting mainly uses the CVSS evaluation model, and the security analyst needs to map the updated expert knowledge to the specified metrics in the CVSS evaluation model.

The evaluation plan based on system asset usage includes sub-tasks system asset data collection, machine learning model training, and system real-time evaluation. Considering the continuity of asset data and the logical relationship within the asset [6], most security analysts use the LSTM model to analyze the input data [7]. In a single task execution scenario, the evaluation error value based on asset usage is only 0.2576. However, in the process of multi-task distributed execution, relying solely on asset usage to evaluate system security will lead to problems of low overall system evaluation accuracy and high false positive rate, which cannot meet the system security evaluation needs of multi-task scenarios.

The current information security system faces the situation of being in an open state and exposed to the complex threat surface for a long time. The traditional evaluation model cannot meet the existing information security system evaluation needs. Artificial intelligence has significant advantages in dealing with massive data, multi-dimensional data, and dynamic data. Therefore, artificial intelligence methods are used to detect abnormal behaviors from massive multi-dimensional data. Although there will be resource overhead in the model training stage, in the real-time detection stage, the detection model can detect malicious behaviors suffered by the infrastructure with a high accuracy rate and achieve an accurate assessment of network infrastructure security. Therefore, the overhead brought by the artificial intelligence method is acceptable.

In evaluation model, vulnerabilities are weaknesses in protected assets that can be exploited. Threats are potential opportunities to compromise information security, and attackers achieve threats by exploiting vulnerabilities in resources and launching attacks. Standards and norms provide guidelines for evaluation. In [8], Tsaregorodtsev et al. implemented cloud infrastructure information security risk assessment based on vulnerability level and usage frequency, however they did not consider real-time threats to the infrastructure. In [9], Yermalovich et al. present a Bayesian-based approach to predicting potential future risks and suggest relying on forecasting the likelihood of an attack on information system assets. However, they do not consider standards and norms. Therefore, in this paper, we propose an AI-based network infrastructure security assessment (ISA-CN) scheme, which concerns China's current fundamental network infrastructure security assessment related standards and specifications and evaluates the object's security states with multi-dimensional automatically monitored network traffic data continuously and comprehensively. Our main contributions are as follows:

- ISA-CN integrates national information security technology standards for multi-dimensional objective comprehensive evaluation.
- ISA-CN combines the dynamic and static judgment methods and proposes the analysis and processing of infrastructure network traffic data based on the deep confidence network, to realize the continuous and automatic analysis of the security state of the network infrastructure.
- ISA-CN uses the analytic hierarchy process to comprehensively evaluate multi-dimensional indicator data.

In the rest of this paper, we summarize related work in Section II, Section III explains the RBF and related standards, introduce the ISA-CN model and concrete construction of our scheme in Section IV and V respectively, present the experimental analysis in Section VI, and offer conclusions in Section VII.

II. Related Work

In this section, we summarize the literature related to our work, including the existing standards, implementation status and network security assessment method.

A. The Existing Standards and Specifications

Regarding the relevant standards for infrastructure security construction, the earliest GB 17859-1999 "Classified criteria for security protection of computer information system" proposed and organized by the Ministry of Public Security in 1999, divided computer information security into 5 levels and proposed the official definition of computer information system[10]. In 2001, GB/T 18336: 2001 "Information Technology Security Technology Information Technology Security Evaluation Criteria" (also known as General Criteria—CC, hereinafter referred to as CC) was promulgated and became the basic criteria for evaluating the security of information technology products and systems. The GB/T 20008-2005 "Information Security Technology—Operating systems security evaluation criteria"[11] and GB/T 20009-2005 "Information Security Technology—Security evaluation criteria for database management system" are formulated with reference to CC [12]. GB/T 19715-2005 "Information Technology—Guidelines for Information Technology Security Management" promulgated in 2005 summarizes previous standards and provides IT security management guidelines rather than solutions[13]. A large number of specifications published in 2006 stipulate that the security analysis of information facilities from different perspectives, such as product performance, encryption technology and facilities.

In 2007, GB/T 20984-2007 "Information Security Technology—Information Security Risk Assessment Specification" made relevant definitions and requirements for risk assessment for the first time[14], and standardized the process of regular security risk assessment for organizations. The GB/T 20985-2007 "Information Technology—Security Techniques—Information Security Incident Management" as a supplement to GB/T 20984-2007 [15], the "System Disaster Recovery Specification" explains the ambiguities in its specific procedures. In 2017, the National Standardization Management Committee issued an instruction to formulate the "Information Security Technology Critical Information Infrastructure Security Assurance Index System" (hereinafter referred to as the index system), which guided the division of indicators in this paper.

B. Network Security Assessment Schemes

Network Security Situation Awareness (NSSA) is a method to evaluate and predict network status by using situation elements obtained from network warning information. In [16], Masduki et al. defined NSSA as “the ability to analyze network information, identify network attacks and evaluate their impact on network systems, measure security risks, and help network administrators make decisions and propose the best way to protect assets”.

There are many methods currently available for the NSSA assessment process. In [17], Shi et al. believe that the network system can be divided into three levels: service, host, and system, and simplify the processing of each level and evaluate the overall security by decomposing the entire system from the bottom to the top. In [18], Wang et al. considered resources such as CPU, memory, hard disk and bandwidth, and used AHP to propose a new method for cloud computing environment resource requirements based on situational awareness.

Researchers begin NSSA research from network attacks. In [19], based on the characteristics of the model proposed by Endsley, Wang et al. proposed a knowledge graph-based network security situational awareness model KG-NSSA (Knowledge-Graph-based NSSA). KG-NSSA combines the asset information of the monitored network and fully considers the monitoring of network traffic, which can effectively reflect specific network attack behaviors and mine attack scenarios. In [20], Yang H et al. proposed a network security situation assessment method based on adversarial deep learning and established an assessment model based on deep autoencoders and deep neural networks. Feature learning using a deep autoencoder model and utilizing a DNN network as an attack classifier. The adversarial training process is constructed by changing the training weights, which improves the detection performance of the model against network attacks, and finally calculates the network security situation value. In [21], Yang et al. proposed a situational awareness method for network attack behavior classification. The model combines the features and strengths of Parallel Feature Extraction Network (PFEN), Bidirectional Gate Recurrent Unit (BiGRU), and Attention Mechanism (ATT). The PFEN module extracts key data from different network attack behaviors.The BiGRU module finds potential representation rules from and from the network attack behaviors. Finally, the network security status values are calculated by combining the severity factors of each attack behavior.

To better assess network security risks, In [22], Yi et al. proposed a network security risk assessment model based on fuzzy theory, particle swarm optimization, and RBF neural network. The assessment of the current network security situation is obtained by mining the laws in the historical data of the network security situation and combining with the current network situation. In [23], Tang et al. combined the randomness and stability of the cloud model, the global search ability and implicit parallelism of the genetic algorithm, and the fast learning ability of the extreme learning machine to design an adaptive cloud improved genetic algorithm optimization. Compared with traditional prediction models, not only the convergence speed is improved, but also the future state of the system can be well predicted.

Considering the antagonism of the two sides of the network attack, In [24], Jia et al. started with attack, defense and network environment, combined attack sequence set, vulnerability set, topology structure set, protection strategy, assets and business elements, introduced uncertainty reasoning model, established capability opportunity intention model, and solved the uncertainty environment security posture calculation problem.

According to the characteristics of massive log information in the system, In [25], Wang et al. proposed a network security situational awareness architecture based on big data. The model detects abnormal behavior of complex attacks by mining log information, realizes active awareness of network anomalies, and improves the overall security situation of the network.

The existing methods have the problem of incomplete evaluation. The network captures data more often while ignoring the corresponding hidden factors in the infrastructure construction. Although the evaluation method in the standard is comprehensive and authoritative, which cannot reflect the security status of facility operation promptly. The method proposed in this paper combines the advantages and disadvantages of the two, it re-division the evaluation indexes. Combining the advantages of new metrics and real-time assessment, we have designed a new assessment framework that is suitable for scenarios where infrastructure is operating clearly and vulnerability patch information is updated in a timely manner.

III. Preliminaries

In the paper, we use the national standards of information security technology and RBM to solve the problem of high subjective dependence in the process of network security situation assessment. Hence, in this section, we formally introduce the key terms used and present the RBM model.

A. Related Standards

The related concepts in this paper come from the three standards of GB/T 31495.3-2015 “Information Security Technology—Information Security Assurance Index System and Evaluation Method” and GB/T 20984-2007 “Information Security Technology—Information Security Risk Assessment Specification” and other information security standard families.

Information security assurance evaluation is conducted around the three dimensions: assurance measures, assurance capabilities, and assurance effects. Assurance measures refer to the assurance needs of stakeholders and the requirements of information security guarantee system construction; assurance capabilities are formed by the interaction of assurance measures, assurance objects and the external environment. Including security protection capabilities, hidden hazard detection capabilities, emergency response capabilities, and information

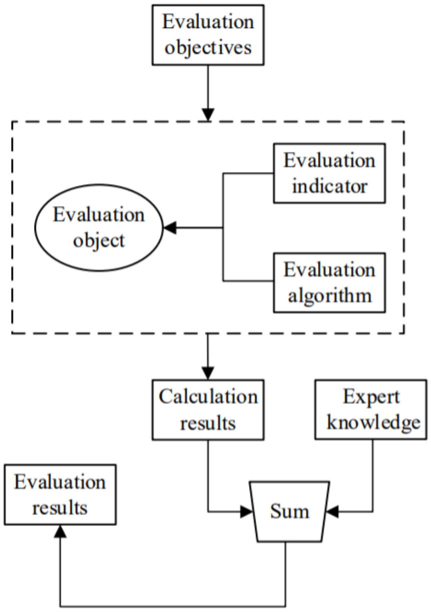

Fig. 1: Elements in Information Security Evaluation

confrontation capabilities; assurance effect is the degree to which the protection capability meets the protection needs of stakeholders after the protection capability acts on the protection object, and provides information for the continuous improvement of the system. The relationship between relevant elements in the evaluation of information security assurance is shown in Fig. 1.

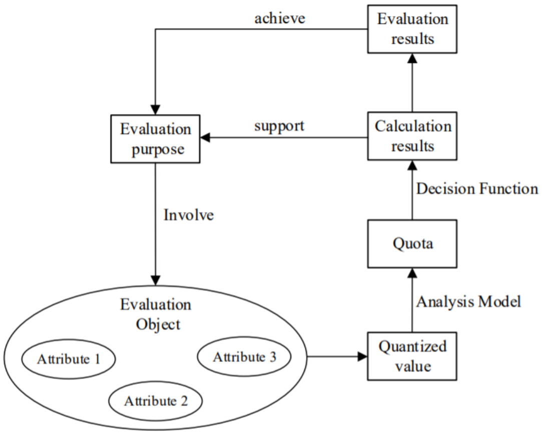

Fig. 2: General Model of Indicator Refinement

The evaluation index is a criterion to measure the level, capability and situation of information security in accordance with the characteristics of the evaluation object and its information security requirements. The general model is shown in Fig. 2. The index level is a structure obtained by decomposing the evaluation content and objects layer by layer. The index level provides guarantee for the orderliness of the index system and provides a framework basis for the construction of the index system.

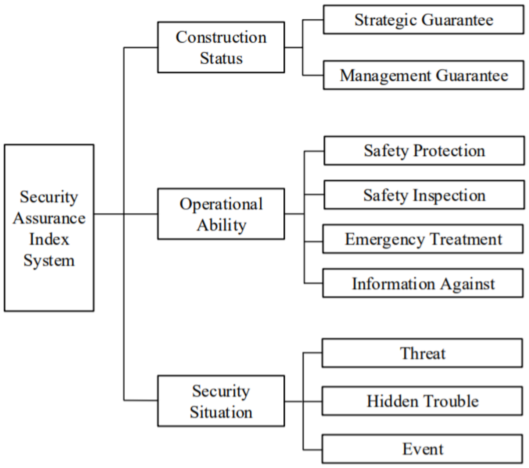

Fig. 3: Critical Infrastructure Security Assurance Index System Framework

According to the indicator framework in GB/T 1495.2-2015, the draft "Information Security Technology Critical Information Infrastructure Security Assurance Evaluation Index System" (hereinafter referred to as the "Draft") proposes a critical infrastructure security indicator system framework, as shown in Fig. 3.

B. Machine Learning Model

Restricted Boltzmann Machine (RBM) is a probabilistic graph model that can be explained by a random neural network. It is proposed on the basis of Boltzmann Machine (BM, Boltzmann Machine). As shown in Fig. 4, RBM contains two layers: a hidden layer and a visible layer. It can be seen from the figure that the neuron connection of RBM has the following characteristics: there is no connection within the layer, and all layers are fully connected, corresponding to a bipartite graph. Unlike BM, RBM requires neurons in the layer to be disconnected, and thus has the following properties: when the state of the visible layer of neurons is given, the activation conditions of the hidden layer neurons are independent; on the contrary, when the hidden layer of neurons is given The state is that the activation of neurons in the visible layer is also conditionally independent.

In RBM, we use E_θ show the Energy Function Matrix Form

$$E_\theta(v,h) = -a^T v - b^T h - h^T W v, \tag{1}$$

where v is the state vector of visible layer, h is hidden layer state vector,a is visible layer offset vector, b is hidden layer bias vector, W is Weight matrix between hidden layer and visible layer.

Use the energy function to give the joint probability distribution of the state, as follows:

$$(v,h) : P_\theta(v,h) = \frac{1}{Z_\theta} * e^{-E_\theta(v,h)}. \tag{2}$$

For practical problems, we are most concerned about the probability distributions$P_\theta(v)$ and $P_\theta(h)$ of the boserved data v,which correspond to the marginal distribution of $P_\theta(v, h)$,which is also called the likelihood function:

$$P_\theta(\theta) = \frac{1}{Z_\theta} * \sum\nolimits_h e^{-E_\theta(v,h)}, \tag{3}$$

$$P_\theta(h) = \frac{1}{Z_\theta} * \sum\nolimits_v e^{-E_\theta(v,h)}. \tag{4}$$

Given a training sample, RBM training means adjusting the parameter θ to fit the given training sample so that the probability distribution represented by the corresponding RBM under the parameter condition conforms to the training data as much as possible. In the training process, the $S = (v_1, v_2, \cdots, v_{n_s})$ is training sample set, $v^i = \left(v_1{}^i, v_2{}^i, \cdots, v_{n_s}{}^i\right)$ is independent and identically distributed training,finnal,we use $L_{\theta,s}$ show the likelihood function to be maximized,$L_{\theta,s}$ expression is as follows:

$$L_{\theta,s} = \prod_{i=1}^{n_s} P(v_i). \tag{5}$$

The Deep Belief Network (DBN) is composed of multiple RBM layers connected in series. It is a neural network that generates a model. By training the weights and biases between neurons in the network, the entire network can generate data according to the maximum probability. Structurally, the deep belief network is composed of a restricted Boltzmann machine and a BP neural network. It is flexible and can be used in conjunction with various neural networks. The output data can represent deeper hidden features and output results has a certain characterization effect on the data. It has been widely used in many fields, but there are few researches on its application in NSSA.

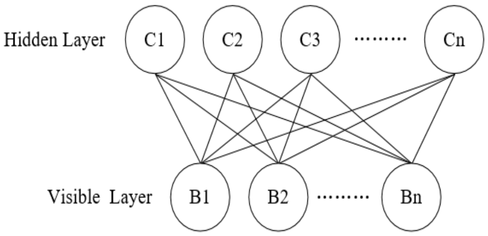

Fig. 4: Basic Structure of RBM

IV. Infrastructure Security Assessment-Chinese National Standards Model Design

In this section, we introduce the three modules of our proposed method in detail.

A. System Architecture

According to the relevant requirements in GB/T 31495.1-2015, the overall structure of security system is shown in Fig. 5. The design goal of this article is a security assurance system, which is responsible for tracking and recording cyber threats and automatically uploading relevant databases of service providers. The security assurance system can also obtain relevant information from the service provider and combine its own algorithms to ensure the security of the infrastructure in real time. The government is responsible for providing relevant and necessary information to the service provider to ensure the stable operation of the security system.

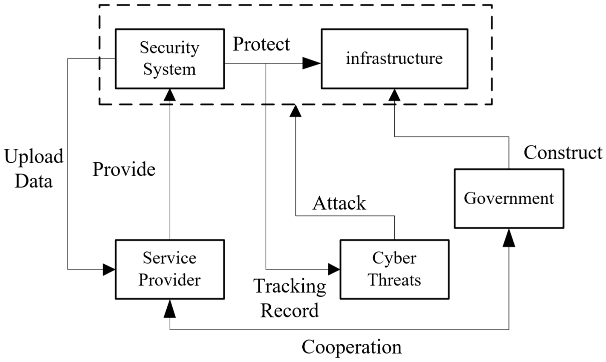

Fig. 5: The Overall Structure of Security System

B. ISA-CN Overview

ISA-CN, an network infrastructure security assessment scheme, integrates China's current fundamental network infrastructure security assessment-related standards and specifications and multi-dimensional data to evaluate the object's security states continuously and comprehensively. Fig. 6 gives an overview of the ISA-CN architecture. It mainly consists of two components: static judgment and dynamic judgment.

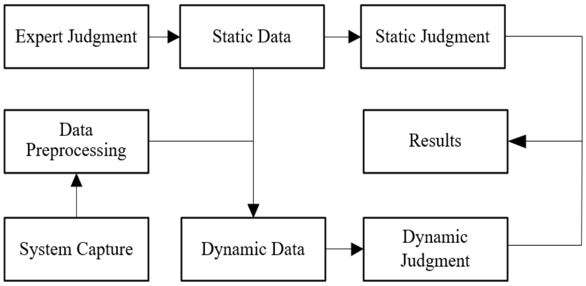

Fig. 6: The Overall System Architecture Model

Static judgment mainly implements infrastructure assessment based on assessment criteria, uses expert knowledge to discriminate, and finally calculates the infrastructure assessment score. The expert score is objective reference data that ensures the objectivity of the final evaluation result.

Dynamic judgment is mainly used to judge the security of the network environment in real-time. However, network traffic data has the characteristics of large data volume, strong representativeness, and strong timeliness, so appropriate sampling frequency and feature selection should be selected during collection. In addition, the dynamic judgment also uses static data as auxiliary indicators.

Finally, ISA-CN combines the static part and the dynamic part to obtain the final judgment result and display the evaluation result.

TABLE I: Basic division of indexes

class	name	index
Construction Status	Planning Index	1
	Institutional Index	2
	Professional Talent Team Index	3
	Capital Investment Index	4
Operational Ability	System-Level Security Evaluation Index	5
	Information Sharing and Reporting Index	6
	Emergency Plan Index	7
	Security Disposal Index	8
	Security Hazard Index	9
Security Situation	Security Threat Index	10
	Unwanted Program Incident Security Posture Index	11
	Security Situation Indicators of Cyber Attack Index	12
	Information Sabotage Event Security Situation Index	13
	Information Content Security Incident Security Index	14
	Catastrophic Event Security Situation Index	15

C. Model Design

The design of the whole judgment system as follows:

- **Static Judgment**

According to GB/T 31495.1-2015 and the relevant indicator evaluation regulations in the draft, it is necessary to regularly conduct security assurance assessment activities for critical infrastructure to ensure its security operation. System operation and maintenance personnel need to count the types and times of network attacks and store the data.

According to the relevant requirements of the draft, as shown in in Fig. 3. ISA-CN divides the indicators into three categories: construction status, operational capability, and security status, where the planning indicators, institutional indicators, professional talent team indicators, and capital investment indicators are divided into construction status categories. System-level security assessment indicators, information sharing and reporting indicators, emergency plan indicators, security disposal indicators, and security threats are divided into operational capability indicators. The security risk index, accidental program event security situation index, network attack security situation index, information destruction event security situation index, content security event security index, and disaster event security situation index are divided into security situation categories, as shown in Table. I. The description of the indicators and evaluation methods are given in Appendix A.

The index vector is denoted as$(\alpha_1, \alpha_2, \cdots, \alpha_{15})$, where the index (the third column in Table. I) is stored in the static data storage segment according to the previous division through the filtering mechanism.

According to GB T 20984-2007 “Information Security Technology Information Security Incident Classification and Classification Guidelines”. ISA-CN assigns the value of assets, then detects and counts abnormal behaviors and finally evaluates the severity of vulnerabilities. The index system can achieve score consistency, that is, the evaluation follows the same score segment, and the score is positively correlated with security.

- **Dynamic Judgment**

The dynamic judgment segment uses the DBN algorithm to implement threat analysis. The DBN algorithm first extracts network traffic data features and normalizes the characteristics, and finally realizes malicious traffic detection. Attacks are usually implemented by exploiting corresponding vulnerabilities. Therefore, according to the relevant provisions in the current draft, vulnerabilities can be used to evaluate security risk indicators, and the relationship between attack behaviors and vulnerabilities can be established. To better reflect the security status of the system, ISA-CN has made the following definitions:

1) Vulnerability Index: The Index value is obtained by fusing the intrusion behavior detected by DBN, the Security Hazaed Index (α_8) and the Security Disposal Index (α_9).
2) Susceptibility Index: The Index value is obtained by integrating Security Threat Index (α_{10}), Unwanted Program Incident Security Posture Index (α_{11}), Security Situation Indicators of Cyber Attack Index (α_{12}), Information Sabotage Event Security Situation Index (α_{13}), Information Content Security Incident Security Index (α_{14}), and Catastrophic Event Security Situation Index (α_{15}).
3) Implied Index: Index that do not directly reflect cyber risk.

It can be found that most of the Construction Status and Operational Ability are Implicited Index, which should be separated from real-time data when making judgments. In addition, there is a correlation between Security Situation and vulnerability severity CVSS (Common Vulnerability Scoring System). Therefore, the indicators are re-divided into three categories:

1) Vulnerability Index: ISA-CN uses the DBN algorithm to detect attack types and then tries to map them to vulnerabilities. If the CVSS value of the vulnerability is unknown, the index value is calculated according to the highest impact level. By looking up the vulnerability

library, ISA-CN determines whether the system has taken countermeasures against the vulnerability. If a countermeasure is taken, the coefficient is set to one, then the Security Disposal Index is taken as the probability of a successful response, and then the Vulnerability Index is obtained. The score in the index system is positively correlated with system security.

2) Susceptibility Index: ISA-CN uses Analytic Hierarchy Process (AHP), where experts give specific weights, weight average their sub-indices, and finally get the Susceptibility Index value. The obtained Susceptibility Index value is used as the system security factor, which is multiplied with the previous Vulnerability Index value to obtain the comprehensive security evaluation value of the system.

3) Implied Index: The Construction Status has great reference value, and the Implied Index value is obtained through the evaluation result of the Construction Status Index. The Implied Index value and the comprehensive security evaluation value are weighted and summed to obtain the final system security evaluation value.

V. Infrastructure Security Assessment-Chinese National Standards Scheme Construction

In this section, we propose a concrete scheme structure based on the Infrastructure Security Assessment-Chinese National Standards Model.

A. Obtain Indexes Values

According to the calculation method given in the draft, calculate or give the relevant index scores according to experience, according to the index in Table I, the index vector is denoted as$(\alpha_1, \alpha_2, \cdot\cdot\cdot, \alpha_{15})$, where the index is stored in the static data storage segment according to the previous division through the filtering mechanism.

Vulnerabilities have CVSS values, which can be divided into three types of evaluation: basic evaluation, environmental evaluation, and life cycle evaluation. Here we only need to use its basic evaluation value, the scale range is 0-10, and it is recorded as c_0.

$(\alpha_5, \alpha_6, \alpha_7, \alpha_8, \alpha_9)$ is a component of Vulnerability Index. According to the result of DBN, judge the intrusion type of the behavior, map the intrusion type to the vulnerability CVSS value, and record the score at this stage as G_0, then $G_0 = C_0$ if the vulnerability corresponding to the attack is found in the vulnerability database at this stage; if the corresponding vulnerability is not found, the attack is judged to be an unrecorded behavior that may cause large losses, they are assigned the highest risk level, that is $G_0 = 10$.

In order to ensure the consistency of the score, $11 - G_0$ is used as the score for this stage. Then multiply the score of this stage by the score of the Security Disposal index α_8, and use this score as the probability value of security disposal. If the first stage successfully corresponds to the vulnerability in the record, the score of the first stage is multiplied by 1, where 1 means that it can be successfully dealt with. According to normal logic, if the threat of vulnerability is low and the probability of being handled safely is high, the system is relatively safe, which shows that the method is consistent with the actual situation. The final score at this stage is recorded as E_0, which is the vulnerability index score.

$(\alpha_{10}, \alpha_{11}, \alpha_{12}, \alpha_{13}, \alpha_{14}, \alpha_{15})$ is a component of Susceptibility Index. In order to synthesize the susceptibility index, AHP is used to assign weights to the index group to obtain the final weight vector $(k_{10}, k_{11}, k_{12}, k_{13}, k_{14}, k_{15})$, then the final assignment expression at this stage is as follows:

$$\begin{aligned} E_1 = (k_{10}, k_{11}, k_{12}, k_{13}, k_{14}, k_{15}) \cdot \\ (\alpha_{10}, \alpha_{11}, \alpha_{12}, \alpha_{13}, \alpha_{14}, \alpha_{15})^T, \end{aligned} \tag{6}$$

where E_1 is the final score of the susceptibility index. $(\alpha_{10}, \alpha_{11}, \alpha_{12}, \alpha_{13}, \alpha_{14}, \alpha_{15})$ is Security Hazard Index, Unwanted Program Incident Security Posture Index, Security Situation Indicators of Cyber Attack Index, Information sabotage event security situation Index, Information Content Security Incident Security Index, Catastrophic Event Security Situation Index, respectively. Then the comprehensive evaluation value of system security E_2 is defined as following:

$$E_2 = E_0 * E_1. \tag{7}$$

The implicit index vector is $(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$, We averaged the 4 scores as the final score because it is relatively independent of the evaluation dimension and cannot directly reflect the degree of safety, written as following:

$$E_3 = \frac{\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4}{4}, \tag{8}$$

where $(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ is Planning Index, Institutional Index, Professional Talent Team Index, Capital Investment Index, respectively.

B. System Security Evaluation Value

The expression of final score E_{fin} is given by the following:

$$E_{fin} = \frac{E_2 + E_3}{12} * 100. \tag{9}$$

The final score range is 0-100, which conforms to the general rules of scoring. After calculating the score, upload the score to the big screen of the situation for the staff's reference. We can set a red line and automatically alarm when the value is lower than the threshold to remind the staff to respond in time.

VI. Experimental Verification

In our section, we introduce the environment and dataset used in our experiment, and analyze our method from the aspects of effectiveness.

A. Experimental Setup

The model training hardware environment in this paper is Intel® Core™ i9-10920X CPU @ 3.50GHz×24, the software environment is PyCharm Community Edition 2021.1.1×64, and the system is Ubuntu 18.04.5 LTS.

This paper uses the NSL-KDD data set, which is obtained by optimizing the KDDCUP99 data set. Features and advantages include: no redundant data; more reasonable control and selection of the number of training sets and test sets; and the number of records at each level of complexity The percentage of records in the original data set is inversely proportional. In the NSL-KDD data set, each row represents a record, and each record contains 41 characteristic parameters and attack types extracted from a connection. The 41 characteristics can be divided into 4 categories: 1. Basic TCP connection characteristics (9 types); 2. TCP connection content characteristics (13 types); 3. Time-based network traffic characteristics (9 types); 4. Host-based Network traffic characteristics (10 types).

B. Experiment analysis

This experiment uses the network structure mentioned in [26] to complete the training, adopts the optimal design, and constructs 3 hidden layers. The structure of the RBM stack is set as (41, 32, 23, 14, 5), and the BP neural network is connected in series at the end of the RBM layer, and the BP network is trained using the output of the RBM layer, and the training set data label and the BP output mean square error are used as the loss function (Loss Function) for training. Unsupervised learning is used for the RBM stack section, and supervised learning is used for the BP section, and the number of iterations is set to 50 times.

Define the number of correctly identified normal data as TN, the number of correctly identified intrusion data as TP, the number of intrusions identified as normal data as FN, and the number of normal data identified as intrusions as TP, then define the Precision Rate as

$$PR = \frac{TN+TP}{TN+TP+FN+FP}, \tag{10}$$

PR cacuate the ratio between the number of correctly predicted points and the total number of points in the test dataset.

False Positive Rate as:

$$FPR = \frac{FP}{TN+FP}, \tag{11}$$

Describe the proportion of negative cases identified as positive cases in all negative cases.

False Negative Rate as:

$$FNR = \frac{FN}{TP+FN}, \tag{12}$$

Describe the proportion of positive cases identified as negative cases in all negative cases.

TABLE II: ISA-CN Results

	Precision	Recall	F1-score
ISA-CN	**97.8%**	**98.5%**	**98.2%**

Table. II, shows the effectiveness of ISA-CN in identifying each attack event for different datasets. For example, the third row shows the training results on the network dataset. The results show that ISA-CN correctly identifies attack behaviors with an average accuracy rate of 97.8%.

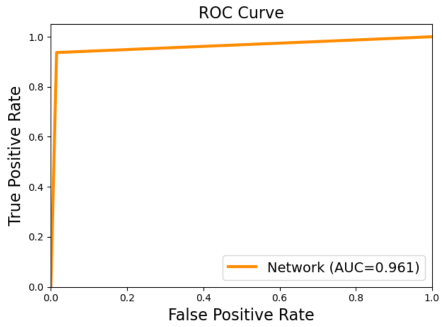

Fig. 7: ISA-CN ROC Curve

The area under the curve (AUC) summarizes the overall position of the entire ROC curve. The ROC curves for ISA-CN are presented in Fig. 7, ISA-CN achieved an average AUC of 96.1%. The number of reported false positives and false negatives identified by ISA-CN was also very low compared to the number of true positives and true negatives.

Next, to verify the effectiveness of the proposed dynamic detection method, we compare it with the commonly used machine learning methods, including RBF, SVM and J48 detection methods. The experimental results of different methods on the NSL-KDD dataset are demonstrated in Table III.

TABLE III: Experimental Results

	PR	FPR	FNR
RBF	94.8%	4.9%	6.9%
SVM	97.4%	0.52%	5.7%
J48	97.6%	0.23%	8.4%
ISA-CN	**97.8%**	**0.5%**	**3.4%**

The results indicate that our proposed dynamic detection method outperforms the current machine learning methods in terms of precision, FPR and FNR. The results also indicate that the dynamic detection method has certain feasibility and superiority in practical applications. For example, through the subsequent training of a large amount of actual scene capture data and continuous adjustment, it is expected to further optimize the parameters and network structure. In this way, the intrusion detection section can achieve better results, and then input the results of intrusion detection into the model, combined with the authority of the model index formulation, to have a certain guarantee for the reliability of the final result.

Compared with the more subjective evaluation method, this model is more optimizable to a certain extent, and in the setting of the index system, it provides the possibility to increase the update frequency of static data, thereby further improving the situation judgment. Scientific and improved emergency response capabilities.

We report the effectiveness of ISA-CN in infrastructure security assessment in Table IV. For example, the first row

TABLE IV: Index Evaluation Score

E_0	E_1	E_2	E_3	E_{fin}
0.17	**0.61**	**0.104**	**0.87**	**8.1**
0.71	0.51	0.36	0.99	10.4
0.57	0.36	0.29	0.90	9.9
0.21	**0.59**	**0.124**	**0.89**	**8.45**
0.65	0.55	0.36	0.89	10.4
0.81	0.69	0.59	0.92	12.5

and four row shows that the E_{fin} is low and may be attacked. Where, E_0 is related to whether the system is attacked. If the vulnerability information corresponding to the current attack is found in the vulnerability library, G_0 is set to the CVSS evaluation value; otherwise, it is set to 10. To ensure the consistency of the scores, $G_0 = 11 - G_0$. Next, if there is a response strategy for the corresponding vulnerability in the database, the evaluation coefficient is set to 1; otherwise, the evaluation coefficient is determined by the Security Disposal Index. Finally, E_0 is obtained through G_0 and the evaluation coefficient, so it can be considered that the current system has been attacked.

The Susceptibility Index E_1 is obtained by the weighted summation of the system security situation index. The weight vector obtained by AHP is $(0.21, 0.08, 0.24, 0.18, 0.19, 0.10)$, and the weighted summation of the weight vector and the Security Situation is obtained to obtain the E_1 value. E_2 is obtained by multiplying E_1 by E_0. The Implied Index E_3 is obtained through the construction index, and the E_{fin} is obtained by summing E_2 and E_3.

VII. Conclusion

In this paper, we propose a new infrastructure operation security situation assessment (ISA-CN) scheme, while it is designed to provide automation and continuity when determining the infrastructure security situation. ISA-CN can extend the linear model to the nonlinear model in subsequent actual operations. As the actual operating conditions become more complicated, this kind of automation, continuity, and optimizable characteristics can provide scientific judgments for infrastructure security situation judgment.

Acknowledgement

This work was supported by the Project of Hainan Province Key Research and Development Program (ZDYF2019202), the Key R&D Program of Shaanxi Province (2021ZDLGY03-10), and the Fundamental Research Funds for the Central Universities (JB210301).

References

[1] National Institute of Standards and Technology. Framework for improving critical infrastructure cybersecurity[J]. Natl. Inst. Stand. Technol., 2014, 1: 1-41.

[2] European Union Agency for Network and Information Security. Methodologies for the identification of Critical Information Infrastructure assets and services[Z]. 2015.2.23.

[3] European Union Agency for Network and Information Security. Stocktaking, Analysis and Recommendations on the protection of CIIs. 2016.1.21.

[4] European Union Agency for Network and Information Security. Technical Guidelines for the implementation of minimum security measures for Digital Service Providers. 2017.2.16.

[5] Zuo X, Chen Z et al. Research on Network Security Evaluation Method Based on Information Security Framework "Golden Triangle Model"[J]. Journal of Adhesion 2020. 41(2): 106-110.

[6] Zhou J, Wang S, Han Y, et al. Model of information system security evaluation based on asset sassociation degree[J]. Computer Engineering and Design. 2017, 38(7): 1691-1696.

[7] Cui M. Research on Key Technologies of Network Security Situation Evaluation and Prediction[D]. China National Knowledge Internet. 2019.1-90.

[8] Tsaregorodtsev A V, Kravets O J, Choporov O N, et al. Information Security Risk Estimation for Cloud Infrastructure[J]. International Journal on Information Technologies & Security, 2018, 10(4): 67-76.

[9] Yermalovich P, Mejri M. Information security risk assessment based on decomposition probability via bayesian network[C]//2020 International Symposium on Networks, Computers and Communications. IEEE, 2020: 1-8.

[10] Classified criteria for security protection of computer information system: GB 17859-1999[S]. Beijing, Office of the Central Cyberspace Affairs Commission, 1999.

[11] Wang L F. Information security technology – Operating systems security evaluation criteria: GB/T 20008-2005[S].Beijing. National Information Security Standardization Technical Committee. 2006.

[12] Zhang B F, Bi H Y, Ye X J, et al. Information security technology—Security evaluation criteria for database management system: GB/T 20009-2005[S]. Beijing: National Information Security Standardization Technical Committee. 2019.

[13] Information technology-Guidelines for the management of IT Security: GB/T 19715-2005[S]. Beijing. National Information Security Standardization Technical Committee. 2005.

[14] Lu K, Zhan B H, Chen Y G, et al. Information security technology—Risk assessment method for information security: GB/T 20984-2007[Ss]. Beijing: National Information Security Standardization Technical Committee, 2018.

[15] Min J H, Zhou Y C, Wang H L et al. Information technology—Security techniques—Information security incident management: GB/T 20985-2007[S]. Beijing: National Information Security Standardization Technical Committee, 2021.

[16] Masduki B W, Ramli K, Salman M. Leverage intrusion detection system framework for cyber situational awareness system[C]//2017 International Conference on Smart Cities, Automation & Intelligent Computing Systems.

IEEE, 2017: 64-69.

[17] Shi L Y, Liu J, Liu Y H, et al. Survey of research on network security situation awareness[J]. Comput. Eng. Appl, 2019, 55(24): 1-9.

[18] Wang J, Li Z, Zhang H. Situation Awareness Based Resource Requirement in Cloud Computing Environment[C]//2017 9th International Conference on Intelligent Human-Machine Systems and Cybernetics. IEEE, 2017, 2: 93-96.

[19] Wang Y, Li Y, Chen X, et al. Implementing Network Attack Detection with a Novel NSSA Model Based on Knowledge Graphs[C]//2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications. IEEE, 2020: 1727-1732.

[20] Yang H, Zeng R, Xu G, et al. A network security situation assessment method based on adversarial deep learning[J]. Applied Soft Computing, 2021, 102: 107096.

[21] Yang H, Zhang Z, Xie L, et al. Network security situation assessment with network attack behavior classification[J]. International Journal of Intelligent Systems, 2022.

[22] Yi B, Cao Y P, Song Y. Network security risk assessment model based on fuzzy theory[J]. Journal of Intelligent & Fuzzy Systems, 2020, 38(4): 3921-3928.

[23] Tang Y, Li C. CGA-ELM: A network security situation prediction model[C]//2021 International Conference on Computer Technology and Media Convergence Design. IEEE, 2021: 58-62.

[24] Jia X, Liu Y, Yan Y, et al. A network security situational awareness approach based on capability opportunity intent model [J]. Application Research Of Computers, Computer Application Research, 2016, 33(06): 1775-1779.

[25] Qian W, Lai H, Zhu Q, et al. Overview of network security situation awareness based on big data[C]//International Conference on Advanced Machine Learning Technologies and Applications. Springer, Cham, 2021: 875-883.

[26] Yu L. Research on intrusion detection based on deep confidence network [J]. Computer Science and Application. 2018, 8(05): 687-701.

Zhaoyang Li Zhaoyang Li is studying for MS degree in computer science and technology in Xidian University, China. His research interests include network security, situational awareness, intrusion detection, and vulnerability scanning in cloud computing.

Hao Duan Hao Duan is studying for MS degree in computer science and technology in Xidian University, China. His research interest includes network security, malicious software detection and cloud computing security.

Jiarui Lei Jiarui Lei is studying for MS degree in computer science and technology in Xidian University, China. His research interest includes network security and the satellite-ground covert communication method based on noise selection.

Zijiang Yang Zijiang Yang, Big Data Architect in ZhongXinDa Information Technology Co., Ltd., Hainan, Haikou. Zijiang Yang received his MS degree in Data Science and Big Data Architecture, from University of Cote d'Azur, Franch. His research interests include hierarchical optimization of data warehouses, ETL, and human portrait algorithm research.

Feng Lin Feng Lin, ZhongXinDa Information Technology Co., Ltd., Hainan, Haikou. received BS degree in Computer Science and Technology, from North University of China. His research interests include network security and cloud computing security.

Yumei Li Yumei Li, ZhongXinDa Information Technology Co., Ltd., Hainan, Haikou. received BS degree in Communication Engineering, from Beijing Electronics Science & technology Institute, China. Her research interest is network security.

Zhiwei Zhang Zhiwei Zhang received his BS degree in network engineering, MS degree in computer systems architecture and PhD degree in Cryptography from Xidian University, China. His research interest includes authentication, access control, data storage security in cloud computing.

APPENDIX

A. Index Details

- **Planning Index.** The Planning Index is used to describe the guiding documents formulated by the information security authorities to lead the overall development of the security of critical information infrastructure. The index value is obtained by evaluating whether to formulate a critical information infrastructure security-related plan and the implementation of the critical information infrastructure security plan.
- **Institutional Index.** The Institutional Index is used to describe all regulatory documents related to critical information infrastructure security, including departmental regulations issued by ministries and local regulations issued by provinces. The index value is obtained by evaluating whether the rules and regulations related to the security of critical information infrastructure have been initially formulated and the implementation of the rules and regulations of the security of critical information infrastructure.
- **Professional Talent Team Index.** The Professional Talent Team Index is used to describe the talent pool of cybersecurity professionals and the cultivation of cybersecurity professionals. The index value is obtained through the proportion of information security professional talent reserve, the proportion of information security practitioners training and the pass rate of information security post ability test.
- **Capital Investment Index.** The Capital Investment Index is used to describe the investment in the security construction of critical information infrastructure. The index value is obtained by evaluating and calculating the growth rate of the critical information infrastructure security budget and the cumulative investment in critical information infrastructure security construction.
- **System-level Security Evaluation Index.** The System-level Security Evaluation Index is used to describe the passing status of critical information infrastructure in the system-level network security protection evaluation. The index value is obtained by calculating the qualified ratio of the three-level information system grade protection evaluation and the four-level information system grade protection evaluation pass ratio.
- **Information Sharing and Reporting Index.** The Information Sharing and Reporting Index are used to record the implementation and coverage of real-time monitoring of critical information infrastructure network security and information sharing. The index data is obtained by calculating the monitoring ratio of the information system, the ratio of the establishment of the information system and the ratio of the early warning system, and the information sharing ratio of the information system.
- **Emergency Plan Index.** The Emergency Plan Index mainly evaluates the emergency drill capability of critical information infrastructure operation and management departments. The index value is obtained by evaluating whether to formulate a critical information infrastructure security emergency plan for the region and the industry, whether to carry out emergency drills on regularly, whether to establish an emergency command coordination mechanism, and whether it has a certain emergency response and recovery ability.
- **Security Disposal Index.** The Security Disposal Index mainly evaluates the ability to deal with security risks such as system vulnerabilities, computer viruses, network intrusions, and network attacks. The index value is obtained by calculating the proportion of handling major information security incidents of critical information infrastructure; the proportion of handling major information security incidents of critical information infrastructure; and the proportion of handling information security incidents of critical information infrastructure being particularly serious.
- **Security Threat Index.** The Security Threat Index mainly evaluates the threats to critical information infrastructure networks. The index value is obtained by calculating the growth rate of the number of attacks on the critical information infrastructure network.
- **Security Hazard Index.** The Security Hazard Index mainly evaluates the security hazards of critical information infrastructure. The index value is obtained by calculating the proportion of critical information infrastructure supercritical security vulnerabilities, the proportion of critical information infrastructure high-risk security vulnerabilities and the proportion of critical information infrastructure critical security vulnerabilities.
- **Unwanted Program Incident Security Posture Index.** The Unwanted Program Incident Security Posture Index mainly evaluates the occurrence of harmful program incidents in critical information infrastructure. The indicator value is obtained by calculating the number of harmful program events that occurred in the key information infrastructure of this unit in the current year and the number of harmful program events that occurred in the key information infrastructure of other units in the current year.
- **Security Situation Indicators of Cyber Attack Index.** The Security Situation Indicators of Cyber Attack Index mainly evaluates the situation of cyber attacks on critical information infrastructure. The index value is obtained by calculating the vertical measurement value of network attack events with larger critical information infrastructure and the horizontal measurement value of network attack events with larger critical information infrastructure.
- **Information Sabotage Event Security Situation Index.** The Information sabotage event security situation Index mainly evaluates the situation of information sabotage events in critical information infrastructure. The index value is obtained by counting the number of information sabotage events of greater or greater magnitude that occurred in the key information infrastructure of the unit in each year and statistics of the number of information sabotage events of the key information infrastructure of other units in the current year.
- **Information Content Security Incident Security Index.**

The Information Sabotage Event Security Situation Index mainly evaluates the situation of information sabotage events in critical information infrastructure. The index value is obtained by counting the number of information sabotage events of greater or greater magnitude that occurred in the key information infrastructure of the unit in each year and statistics of the number of information sabotage events of the key information infrastructure of other units in the current year.

- **Catastrophic Event Security Situation Index.** The Catastrophic Event Security Situation Index mainly evaluate the record situation of catastrophic events of critical information infrastructure networks. The index value is obtained by calculating the number of catastrophic events with a larger or greater magnitude that occurred in the key information infrastructure of the unit each year and the number of catastrophic events with a larger or larger magnitude that occurred in the key information infrastructure of other units in the current year.