Article

Risk Assessment Method for Edge Intelligence Control Platforms Based on Hybrid Game Theory

Chuan He , Bo Zhang * , Tao Zhang , Ze-Sheng Xi , Yun-Fan Wang

Posted Date: 26 February 2025

doi: 10.20944/preprints202502.2083.v1

Keywords: edge intelligence control platforms; hybrid game theory; risk assessment; fuzzy analytic hierarchy process (FAHP); CRITIC method; attack tree model

Article

Risk Assessment Method for Edge Intelligence Control Platforms Based on Hybrid Game Theory

Chuan He, Bo Zhang *, Tao Zhang, Ze-Sheng Xi and Yun-Fan Wang

State Grid Laboratory of Power Cyber-Security Protection and Monitoring Technology, China Electric Power Research Institute Co., Ltd., Nanjing, China

* Correspondence: zhangbo6@epri.sgcc.com.cn

Abstract: Risk assessment techniques have been widely used in edge intelligent control platforms from security protection to decision optimization. In recent years, many researchers have applied machine learning or deep learning to risk assessment in edge intelligent control platforms. However, these approaches face significant challenges, including high computational resource requirements, high data dependency, and poor interpretability. In this paper, we propose a risk assessment method for edge intelligent control platforms based on hybrid game theory, which constructs a two-dimensional security risk assessment framework across cyber and physical domains. The attack tree model is first utilized to meticulously outline the potential attack paths and integrate the mixed-strategy game between attackers and defenders at the leaf nodes. Then, through game-theoretic analysis, the payoff functions of both parties are established, Nash equilibrium is determined to predict strategic choices, and the fuzzy analytic hierarchy process (FAHP) is combined with the CRITIC weighting method to quantify the risk associated with each node in the attack tree model. Finally, the risk values of the root nodes are aggregated to assess the overall security level of the platform. This approach effectively simulates real-world adversarial interactions and improves the accuracy and practicality of risk assessment.

Keywords: edge intelligence control platforms; hybrid game theory; risk assessment; fuzzy analytic hierarchy process (FAHP); CRITIC method; attack tree model

1. Introduction

As edge intelligent control platforms are widely used in critical areas such as industrial IoT and smart grids, the issue of their security is critical. Platforms face potential threats such as cyber-attacks, data tampering, and system failures during data processing and decision-making, and these problems may lead to serious economic losses or even jeopardize public safety. Risk assessment methods play a central role in safeguarding platform security by identifying, quantifying and predicting potential threats, providing a scientific basis for formulating protective measures, which not only improves the system's ability to defend against known threats, but also identifies unknown risks in advance through predictive analysis. Risk assessment is particularly important in edge intelligence platforms, which can dynamically identify the risk posture of edge nodes in distributed environments and optimize security policies, so as to achieve a balance between performance and security, and ensure efficient and stable system operation.

Traditional risk assessment methods have gone through several stages such as rule-based, quantitative analysis and empirical judgment. However, they are unable to cope with rapidly changing attack patterns because they lack the ability to adapt to complex and dynamic environments and are difficult to update and adjust in real time. In addition, traditional methods are also incompetent in dealing with the security risks of edge intelligent control platforms, mainly because edge platforms cannot provide efficient, real-time risk assessment and policy optimization due to limited resources, dynamic environment and heterogeneous data.

In recent years, researchers have introduced Deep Learning (DL) into the study of risk assessment 1. Using the advantages of deep neural networks in feature extraction and pattern recognition, researchers have developed intelligent assessment models for cyber attack detection, fault diagnosis and threat prediction. These models are able to automatically extract key risk features through learning from massive historical data, enabling more efficient threat identification and risk quantification. These show strong advantages in dealing with systems such as edge intelligent control platforms, which are resource-constrained, environmentally dynamic, and data heterogeneous.

Current risk assessment methods based on deep learning can be categorized into three main types: supervised learning, unsupervised learning and reinforcement learning.

Supervised learning mainly predicts and assesses risk events by training labeled data through deep neural networks 2, and such methods have the advantage of being able to learn accurate risk prediction models through labeled data, but face the problem of high data labeling costs. Unsupervised learning is widely used in areas such as anomaly detection and fraud identification by analyzing the intrinsic structure of unlabeled data 3. Self-encoders and clustering algorithms have achieved some results in these tasks, especially performing well when data labeling is difficult, but they face the problems of difficult model evaluation, sensitivity to data noise, and lack of interpretability in risk assessment. Reinforcement learning, on the other hand, focuses on learning optimal decision-making strategies through interaction with the environment 4, and is suitable for dynamically changing risk environments, especially for real-time risk assessment and decision optimization in complex systems. Despite the high adaptability of reinforcement learning in complex scenarios, the demand for large-scale data and computational resources is high, and the following challenges still exist in specific implementation:

(1) High computational resource requirements: Deep learning typically requires huge computational resources and storage, which may not be feasible for resource-constrained environments such as edge intelligent control platforms. Especially when deploying these models on edge devices, computational power and memory constraints may affect the efficiency and real-time performance of the models.

(2) High data requirements: Deep learning and reinforcement learning rely on huge high-quality data for training. In many real-world applications, especially when facing new or unknown attack patterns, obtaining sufficient data for effective training is a challenge. In addition, the heterogeneity between different data sources may also increase the difficulty of data processing and fusion.

(3) Poor model interpretability: Deep learning models have poor interpretability. In security risk assessment, the lack of interpretability can undermine trust in assessment outcomes and complicate the task of tracing and troubleshooting the model's decision-making process during anomalies.

Therefore, in order to make up for the limitations of conventional risk assessment methods, this paper proposes a risk assessment method based on hybrid game theory for edge intelligent control platforms, which is applied to edge intelligent control platforms, and the main contributions are as follows:

(1) A hierarchical risk analysis method based on the attack tree model is proposed, which reduces the global computational complexity by constructing the element hierarchy in the information and physical domains and decomposing the global complex problem into local subtasks. In each sub-task, only the local strategy selection and risk assessment need to be analyzed, and the end node introduces the mixed game strategy of attack and defense, and the optimal strategy is obtained by solving the Nash equilibrium point through the finite-dimensional payoff function, which effectively alleviates the high computational resource demand.

(2) A risk quantification method combining fuzzy hierarchical analysis (FAHP) and critical synthesis assignment method (CRITIC) is proposed, which improves the model adaptability through the weighted processing of multi-source heterogeneous data by FAHP and CRITIC, and does not require large-scale labeled data or high-quality samples, which effectively solves the problem of high data demand.

(3) An interpretable attack tree-game theory framework is proposed to visualize the attack path and hierarchical structure through the attack tree model, so that the source of risk is clearly visible. The game theory analysis defines the payoff functions of both attackers and defenders, and solves the Nash equilibrium to clarify the optimal strategy. Combining FAHP and CRITIC generates transparent and traceable risk values and weight assignments, which provide a clear basis for root node risk assessment and enhance the interpretability and reliability of the model.

2. Related Work

Edge intelligent control platforms are rapidly developing under the impetus of IoT and 5G communication technologies, and their applications in industrial automation, smart cities, telemedicine, and other fields are increasing 12. Edge computing effectively reduces latency and improves responsiveness by relocating data processing and analysis tasks near the data source, which is pivotal for realizing the infrastructure of smart cities. For example, edge computing enables real-time processing of traffic flow data to optimise traffic light control, reduce congestion and improve road usage 56. Edge computing can also support communication between self-driving vehicles to ensure driving safety 7. In addition, this technology holds significance in the energy management of smart buildings by automatically adjusting the working status of facilities such as air conditioning and lighting through in-depth analysis of the collected data to achieve energy savings and reduce emissions 8. In the field of security monitoring, edge intelligent surveillance systems can analyze video streams in real-time, which can quickly identify abnormal behaviours and thus enhance public safety protection 9.

In the field of telemedicine, edge intelligent control platforms provide real-time and efficient healthcare services to patients by integrating IoT devices, AI technologies and edge computing capabilities. For example, through edge computing technology, health monitoring devices installed in patients' homes can collect health data in real-time and perform preliminary analysis and processing through edge servers to detect potential health problems and issue alerts in a timely manner 1011. In addition, edge intelligence can also support remote surgery and diagnosis, enabling doctors to remotely operate medical devices or conduct condition analysis through high-definition video transmission and real-time data exchange to provide timely and effective treatment plans for patients 12. In terms of chronic disease management, the edge intelligence control platform can help doctors formulate personalised treatment plans and effectively control the development of the disease through continuous monitoring of the patient's physiological parameters, combined with AI algorithms for data analysis and disease prediction 13.

In the realm of industrial automation, edge intelligent control platforms enhance data handling capabilities by relocating computing power from the cloud to the network's edge. In industrial robotics systems, edge computing enables faster real-time response and network transmission performance, thus improving productivity and product quality 14. In addition, edge intelligence can be applied to monitor the condition and perform predictive maintenance on industrial equipment, thereby minimizing downtime and repair costs through the analysis of sensor data, which enables timely detection of equipment failures and trends of performance degradation [15]. In the smart manufacturing process, edge intelligence control platforms are also able to support highly personalised production processes, adjusting production parameters based on real-time data to achieve efficient customised production 16.

In addition to this, edge computing is widely used in the fields of agriculture and environment monitoring and security and privacy protection. In the field of agriculture and environment monitoring, edge computing can be used to collect and analyse sensor data in real-time, such as soil moisture, temperature, light intensity, etc., to optimize the agricultural production process and protect the natural environment 6. Edge computing plays a pivotal role in enhancing security and privacy safeguards by locally encrypting and filtering data, mitigating the chances of unauthorized data exposure and safeguarding users' confidentiality 1718.

While the distributed architecture of edge intelligent control platforms brings the benefits of low latency and high efficiency, it also faces a number of security challenges. The decentralised deployment characteristics of edge devices make them more vulnerable to physical attacks, illegal intrusion and data tampering. This, coupled with the limited resources of edge devices, makes it difficult for traditional security protection mechanisms to effectively cover them, resulting in platforms facing risks such as external malicious attacks (e.g., DDoS attacks, man-in-the-middle attacks), internal security vulnerability exploits, data leakage, privacy violations, and supply chain security threats. Current risk assessment methods, including traditional security audits, static risk assessment models, or simple quantitative analysis methods, have some limitations. These methods tend to ignore the dynamically changing threat scenarios in the edge computing environment and lack the ability to dynamically monitor and respond to real-time threats. In addition, the assessment models may be oversimplified and are usually based only on historical data or static rules, making it difficult to accurately reflect complex system interactions and changes in attacker behaviour. The assessment process does not have a sufficient understanding of the causal relationships of security events and ignores the strategic interactions between attackers and defenders, resulting in assessment results that may not be sufficiently accurate. At the same time, existing methods often neglect the cost-benefit analysis of security measures and fail to comprehensively consider the economic factors of risk management.

In view of these limitations, there is an urgent need to develop a new risk assessment methodology, which should be able to comprehensively consider system dynamics, and strategic interactions between attacking and defending parties, and incorporate the characteristics of edge computing in order to enhance the timeliness, accuracy, and practicality of risk assessment. Based on existing research, this paper proposes a hybrid game-based risk assessment method for edge intelligent control platforms, which integrally considers system dynamics and environmental uncertainty, while adopting the distributed architecture of edge computing to achieve fast response and local optimisation. By introducing game theory to model the interactions between participants, the approach is able to assess and balance the benefits and risks of different participants under uncertainty conditions. In addition, by leveraging the swift data processing and robust connectivity capabilities of edge computing, the method enables real-time and precise risk assessment, thereby enhancing the overall security and reliability of the system.

3. Methodology

3.1. Overall Architecture

In constructing a security risk assessment system for edge intelligent control platforms, this study first establishes a hierarchy of elements containing both information and physical domains, which provides a theoretical basis for comprehensively identifying and analysing security risks. Subsequently, an attack tree model is used to reveal the potential attack paths of the platform, and a hybrid attack-defence game strategy is embedded in the end node of the model to simulate the dynamic game process between the attacker and the defender.

Further, through the analysis of game theory, the payoff functions were defined, and the Nash equilibrium point was solved to predict the probability of occurrence of the attack behaviours under different defence strategies, which provided decision support for the selection of defence strategies. In addition, the risk value of each leaf node in the attack tree is precisely quantified by combining the fuzzy hierarchical analysis and Critic comprehensive assignment method, which ensures the scientificity and rationality of risk assessment.

Ultimately, the attack tree approach is utilized to determine the risk associated with the root cause, allowing for a comprehensive evaluation of the security risk level within the edge intelligent control system. This assessment offers both theoretical insights and practical advice for developing effective security safeguards. The methodological framework of this research enhances the precision of security risk assessment while offering a fresh perspective on security protection strategies within the edge computing environment.

3.2. Construct Hierarchical Diagrams

The information domain and physical domain in the edge intelligent control platform are analysed for security, and the assessment elements are summarized to derive the security risk assessment elements of the edge intelligent control platform. The information domain is mainly assessed in four aspects of security, including terminal device security, authentication service security, access control security, and communication security, which mainly include vulnerability detection and removal, malicious code detection and removal, online update, software fault tolerance and attack resistance; configuration management, session management, and identity authentication; user access control, information access control, and service access control; and communication integrity and communication confidentiality, for a total of 15 security assessment elements. The physical domain is mainly assessed from three aspects of physical equipment security, physical environment security, and physical interface security, which mainly includes equipment reinforcement measures, physical access control, environmental security (e.g., fire prevention, waterproofing, and anti-theft, etc.); disaster protection (e.g., earthquakes, floods, etc.), power supply stability, humidity control, and temperature control; and interface protection mechanisms, physical interface security, interface access control, etc., with a total of 10 security assessment elements 19. Construct the above elements into a security risk assessment element hierarchy diagram. The diagram is illustrated below.

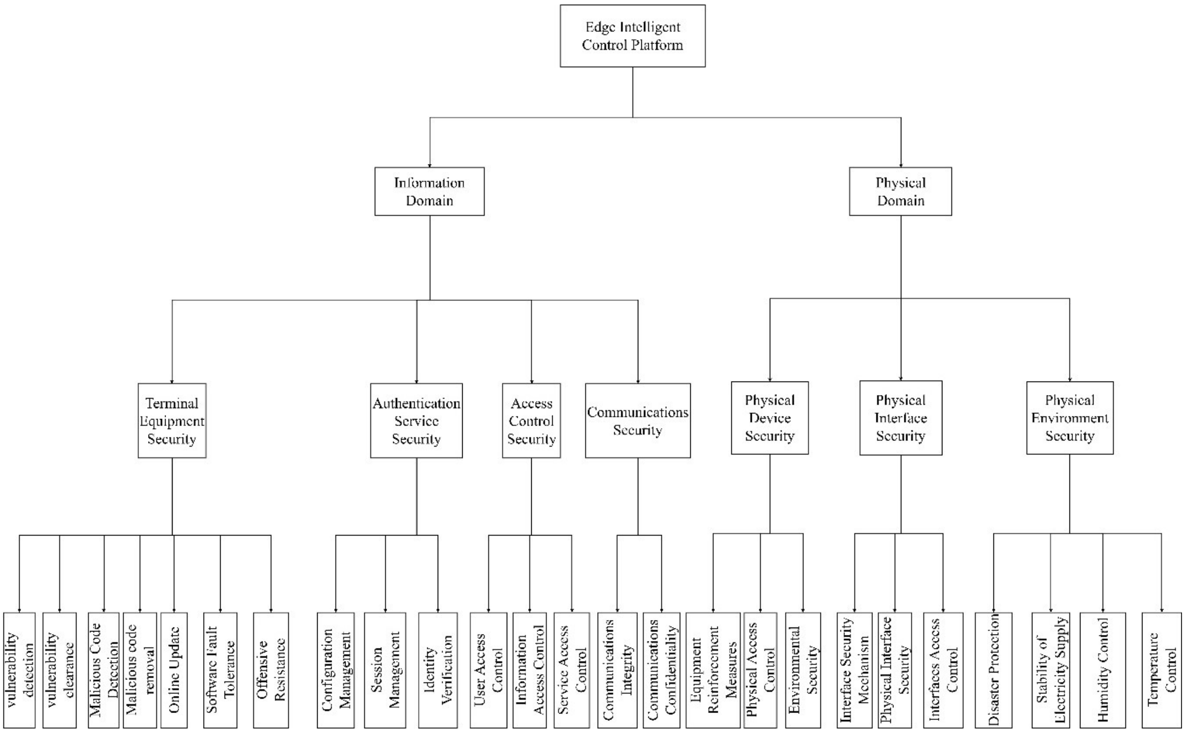

Figure 1. Hierarchical Structure of Security Risk Assessment Elements Including Information Domain and Physical Domain Based on Edge Intelligent Control Platform.

4. Experiments

4.1. Attack Tree Game Theory Convergence Assessment

4.1.1. Modelling the Attack Tree

First, critical assets and potential security targets of the edge intelligent control platform are identified, which become the root nodes of the attack tree. Next, possible means and methods of attack are analysed and these are added to the attack tree as intermediate nodes. These intermediate nodes represent the possible strategies and steps that the attacker may take to achieve the goal. Further, each intermediate node is refined to unfold specific attack behaviours or conditions to form leaf nodes. In these leaf nodes, attack and defence hybrid game strategies are introduced, mimicking the interactive decision-making dynamics between the attacker and the defender. The attacker will consider potential defences when choosing an attack path, while the defender will optimise its own defence strategy based on the potential behaviour of the attacker.

In this process, the construction of an attack tree model is required. To comprehensively assess risks associated with the edge intelligent control platform, it is essential to consider both the information and physical domains. Therefore, modeling is required at three distinct levels: the physical tier, the transmission tier, and the decision-making tier. Assuming that the entire Edge Intelligent Control Platform consists of ns sensors, nh controllers and na actuators, abstracting these Edge Intelligent Control Platform components with the network vulnerabilities they have as Sensor Nodes, Controller Nodes and Actuator Nodes collaborate in modeling the Edge Intelligent Control Platform, which comprises a variety of nodes as follows:

$$\boldsymbol{s} = \left\{s_1, s_2, \ldots, s_{ns}\right\} \tag{1}$$

$$\boldsymbol{h} = \left\{h_1, h_2, \ldots, h_{nh}\right\} \tag{2}$$

$$\boldsymbol{a} = \left\{a_1, a_2, \ldots, a_{na}\right\} \tag{3}$$

In the Edge Intelligent Control Platform, the attack tree structure is designed as shown in Figure 2. The root node is for the normal operation of the whole platform, the intermediate nodes are abstracted from the 'with' 'or' relationship, encompassing the controller layer, actuator layer, and sensor layer. Meanwhile, the leaf nodes signify the physical components involved in a specific attack event, i.e., the sensors that the attacker may attack, actuator or controller node that the attacker may attack. The 'with' node satisfies the attack condition if and only if all branches of the 'with' node are successfully attacked; and as long as a branch under the 'or' node is successfully attacked, the 'or' node will be attacked. The 'or' node satisfies the attack condition as long as one branch under the 'or' node is successfully attacked. In these leaf nodes, hybrid attack-defence game strategies are introduced, mimicking the strategic interactions and decisions exchanged between the attacker and the defender. The attacker will consider potential defences when choosing an attack path, while the defender will optimise its defence strategy based on the potential behaviour of the attacker 20.

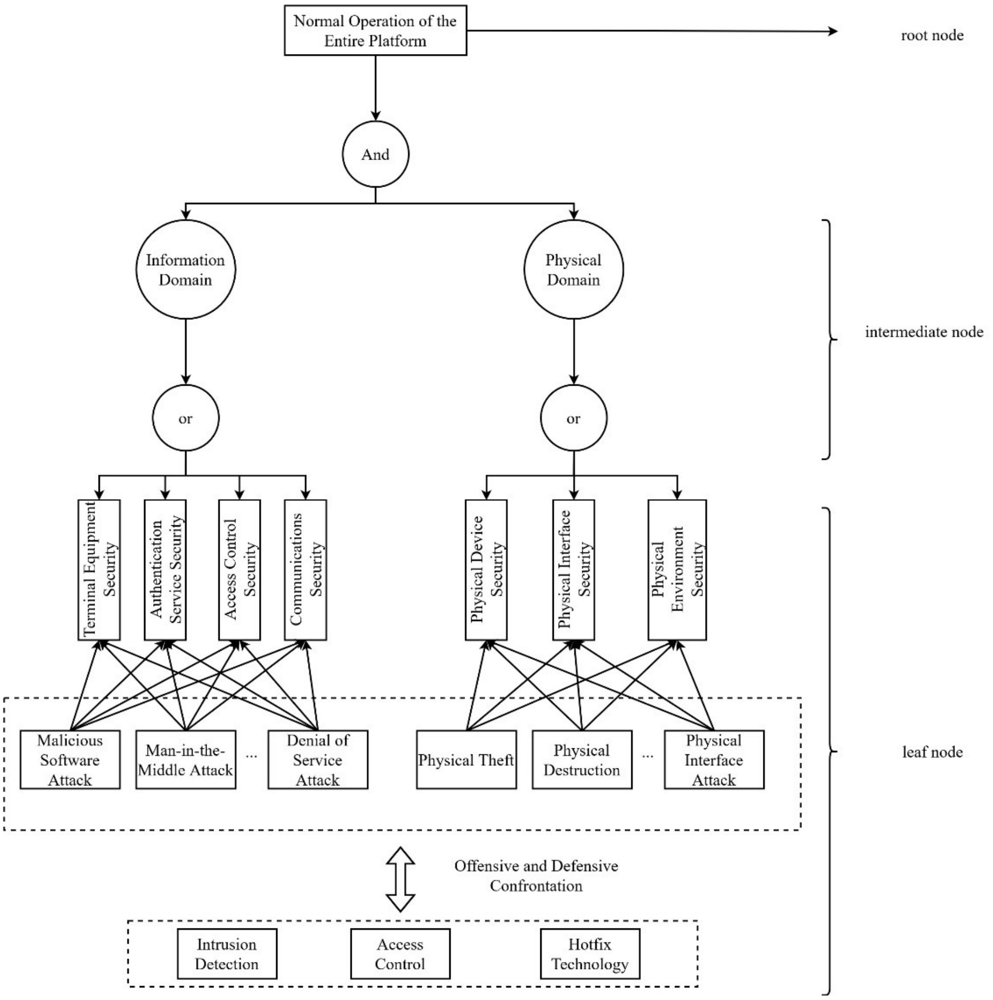

Figure 2. Attack Tree Model of Edge Intelligent Control Platform.

In the attack tree, a hybrid strategy combining both attack and defense is integrated into the leaf nodes 21, enabling the simulation of the game between the attacker and the defender.

4.2. Game-Theoretic Nash Equilibrium Defence Strategy Probability Analysis

Define the attack and defence game models at the terminal nodes of the attack tree:

$$ADGM=\left\{\boldsymbol{O},\boldsymbol{V},\boldsymbol{\pi},\boldsymbol{Z}\right\} \tag{4}$$

Where, $\boldsymbol{O}=\left(O_{At},O_{De}\right)$, denotes the participant who masters multiple activities in the game, the subscript At denotes the attacker, and the subscript De denotes the defender; $\boldsymbol{V}=\left\{V_{At},V_{De}\right\}$, where $V_{At}=\left\{v_{At}^{1},v_{At}^{2},\ldots,v_{At}^{m}\right\}$, $V_{De}=\left\{v_{De}^{1},v_{De}^{2},\ldots,v_{De}^{n}\right\}$, m denotes the attacker's possible m kinds of attacking actions in the course of the game, and n denotes the defender's possible n kinds of defending actions in the course of the game; $\boldsymbol{\pi}=\left\{\pi_{At},\pi_{De}\right\}$denotes a specific decision made by the attacker and the defender during the game, if multiple actions are distributed with a certain probability as a mixed strategy, then $\pi_{At}=\left\{p\left(v_{At}^{1}\right),p\left(v_{At}^{2}\right),\ldots,p\left(v_{At}^{m}\right)\right\}$, $p\left(v_{At}^{m}\right)$ is the probability that the attacker performs a certain action, $\pi_{De}=\left\{p\left(v_{De}^{1}\right),p\left(v_{De}^{2}\right),\ldots,p\left(v_{De}^{n}\right)\right\}$, $p\left(v_{De}^{n}\right)$is the probability that the defender performs a certain action; $\boldsymbol{Z}=\left(Z_{At},Z_{De}\right)$denotes the rewards forthe two opposing sides at the conclusion of a game vary based on the strategies employed. Furthermore, if the game involves mixed strategies, then $\boldsymbol{Z}$ is in the form of a payoff matrix.

Constructing different attack and defence gain function calculations is defined as follows:

(1) Establish the defender's benefit function, which quantifies the defender's payoff and is calculated as follows:

$$RF_D = (1-\vartheta)\times(1-\upsilon)SL - \vartheta SL - DR \tag{5}$$

Where ϑ is the success rate of different attack methods against different defence methods, $1-\vartheta$ is the probability of success of such defence methods, υ is the gain factor of the indirect return gained from the failure of such attack methods, DR represents the cost of the defence methods, i.e., the cost of adopting a certain defence method, and SL is the loss that may be caused by the attack method corresponding to the defence method at this time. The gain function for a defence method is obtained by subtracting the gain from the success of this defence method from the gain from the attack if the defence fails, and subtracting the cost of this defence.

(2) Define the attacker gain function RF_A, which represents the attacker's gain and is calculated as follows:

$$RFA = \vartheta SL - (1-\vartheta)\upsilon SL - AR \tag{6}$$

Where ϑ is the probability of success of such an attack, represents the cost of the attack, i.e., the cost of employing a particular attack, and υ is the payoff factor of the indirect payoff gained by the failure of such an attack. The profit function for an attack method is calculated by subtracting the indirect benefits of a failed attack and the cost of the attack from the rewards of a successful attack.

Determining the payoff functions of the attacker and the defender allows for the solution of the unfolding attack-defence game. The Nash equilibrium is solved for the probability probabilities of the decisions of all participants. In the Edge Intelligent Control Platform game, the assailant and the guardian each take their optimal strategies to form a strategy combination (π_{At}^*, π_{De}^*), where π_{At}^* is the assailant's optimal counter-strategy against the defender's strategy π_{De}^*, and π_{De}^* signifies the guardian's best defensive response against the assailant's strategy π_{At}^*, i.e., for any $p(\nu_{At}{}^m)\in\pi_{At}$, $p(\nu_{De}{}^n)\in\pi_{De}$, is satisfied:

$$\begin{aligned} Z_{At}(\pi_{At}^*, \pi_{De}^*) &\geq Z_{At}(p(\nu_{At}{}^m), p(\nu_{De}{}^n)) \\ Z_{De}(\pi_{At}^*, \pi_{De}^*) &\geq Z_{De}(p(\nu_{At}{}^m), p(\nu_{De}{}^n)) \end{aligned} \tag{7}$$

Therefore strategy (π_{At}^*, π_{De}^*) is a solution to the Nash equilibrium of the offensive and defensive game model $ADGM$.

For the mixed-strategy model, the game actions of the attacker and the strategist are a probability distribution, and if the attacker's strategy is $\pi_{At} = \{p(\nu_{At}{}^1), p(\nu_{At}{}^2), \ldots, p(\nu_{At}{}^m)\}$, and the the guardian's tactical approach is $\pi_{De} = \{p(\nu_{De}{}^1), p(\nu_{De}{}^2), \ldots, p(\nu_{De}{}^n)\}$, the payoff functions (Z_{At}, Z_{De}) for both the assailant and the guardian, when considering mixed strategies, will constitute a payoff matrix.

$$Z_{At} = \begin{pmatrix} z_{At11} & \cdots & z_{At1n} \\ \vdots & \ddots & \vdots \\ z_{Atm1} & \cdots & z_{Atmn} \end{pmatrix}, Z_{De} = \begin{pmatrix} z_{De11} & \cdots & z_{De1m} \\ \vdots & \ddots & \vdots \\ z_{Den1} & \cdots & z_{Denm} \end{pmatrix},$$

where,e, z_{Denm} denote the respective gains for the assailant and the guardian after selecting the respective attack and defence methods. For both the attacker and the defender, the overall expected gain function is:

$$Z_{At}(p(\nu_{At}{}^i), p(\nu_{De}{}^j)) = \sum_{i=1}^{m}\sum_{j=1}^{n} p(\nu_{At}{}^i)p(\nu_{De}{}^j)z_{Atij} \tag{8}$$

$$Z_{De}(p(\nu_{At}{}^i), p(\nu_{De}{}^j)) = \sum_{i=1}^{m}\sum_{j=1}^{n} p(\nu_{At}{}^i)p(\nu_{De}{}^j)z_{Deji} \tag{9}$$

Where $p(\nu_{At}{}^i)$ describes the probability that the assailant choose a specific attack behavior i and $p(\nu_{De}{}^j)$ denotes the probability that the defender picks behaviour j.

If the following two equations hold for any $p\left(v_{At}{}^{i}\right)$ and $p\left(v_{De}{}^{j}\right)$, then $p_{*}=\left(p\left(v_{At}{}^{*}\right),p\left(v_{De}{}^{*}\right)\right)$ is called a solution of the mixed strategy Nash equilibrium, where $p\left(v_{At}{}^{*}\right)$ can be regarded as the attacker's probability prediction of his behaviour, indicating which attack method the attacker may adopt, and $p\left(v_{De}{}^{*}\right)$ represents the defender's probability prediction of his behavior, i.e., the defender's possible defence method.

$$Z_{At}\left(p\left(v_{At}{}^{*}\right),p\left(v_{De}{}^{j}\right)\right)\geq Z_{At}\left(p\left(v_{At}{}^{i}\right),p\left(v_{De}{}^{j}\right)\right) \tag{10}$$

$$Z_{De}\left(p\left(v_{At}{}^{i}\right),p\left(v_{De}{}^{*}\right)\right)\geq Z_{De}\left(p\left(v_{At}{}^{i}\right),p\left(v_{De}{}^{j}\right)\right) \tag{11}$$

4.2. Combined Fuzzy Hierarchical Analysis and Critic's Method for Assigning Attack Tree Risk Assessment

4.2.1. Fuzzy Hierarchy Analysis

To correctly assess the influence of various defence modalities on leaf nodes, a blend of subjective and objective approaches is used to ascertain the significance of each defence modality and to overcome the limitations of a single assignment.

Fuzzy hierarchical analysis represents an evolution of the traditional hierarchical analysis (AHP). It mainly solves the problem of weight allocation in the decision-making process when the evaluation factors are affected by subjective judgement and uncertainty. FAHP allows decision makers to use fuzzy language to express evaluation opinions 22, such as ‘slightly important’, ‘very important’, etc., so that qualitative evaluation can be transformed into quantitative data, enhancing the flexibility and realism of the decision-making process. Qualitative evaluation is transformed into quantitative data, thereby enhancing the adaptability and realism of the decision-making procedure.

The procedure for implementing the FAHP involves the following steps:

(1) Determine the evaluation indicators and hierarchy. First, based on the characteristics and potential threats of the edge intelligent control system, the specific elements of the evaluation are defined, such as the danger of data breaches, threats to physical security, and risks of access control. Construct an evaluation hierarchy, which usually includes a target layer (e.g., overall platform security), a criterion layer (e.g., the effectiveness of security control measures), and an indicator layer (e.g., soundness of specific security configurations).

(2) Establishment of a hierarchy model. Based on the hierarchy diagram determined in the previous step, a hierarchy model is established, i.e., each factor is arranged into multiple levels in descending order, and a hierarchy containing guidelines, sub-criteria and leaf nodes is formed.

(3) Establishment of judgement matrix. For the relationship between each level, using the 0.1-0.9 nine scale method, a judgement matrix is established, resulting in the construction of a fuzzy judgement matrix denoted as $\mathbf{A}=\left(a_{ij}\right)_{n\times n}$. As illustrated in Table 1. If the elements in the fuzzy matrix $\mathbf{A}$ adhere to the equation $a_{ij}+a_{ji}=1$, then $\mathbf{A}$ is deemed a fuzzy complementary matrix at this time.

(4) Establish a fuzzy consistency matrix. Firstly, the fuzzy complementary discriminant matrix $\mathbf{A}$ is built, and then its consistency test is carried out, which is finally transformed to the fuzzy consistency matrix $\mathbf{R}$ .When comparing two factors, the subjectivity of the judgement and the complexity of the issue affects the need for a consistency test of the discriminant matrix to guarantee the accuracy of the evaluation outcomes. Then, each row of the fuzzy complementary matrix $\mathbf{A}$ is summed to obtain a fuzzy consistency matrix $\mathbf{R}=\left(r_{ij}\right)_{m\times n}$, i.e. $\mathbf{r}_{i}=\sum_{k=1}^{n}a_{ik}$ $\left(i=1,2,\ldots,n\right)$, and through the process of mathematical transformation $\mathbf{r}_{ij}=\dfrac{r_i-r_j}{2\left(n-1\right)}+0.5$, the matrix $\mathbf{R}$ is obtained.

Table 1. Nine Scale Quantity Scale of 0.1-0.9.

judgment scale	Meaning and explanation
0.5	equally important the two influences are equally important in comparison
0.6	slightly important one element holds slightly greater importance compared to the other when comparing the two influencing factors
0.7	more important one element holds more greater importance compared to the other when comparing the two influencing factors
0.8	very important one element holds considerably greater importance in comparison to the other when comparing the two influencing factors
0.9	extremely important one element holds extremely greater importance in comparison to the other when comparing the two influencing factors
0.1 0.2 0.3 0.4	inverse comparison When element a_i is compared with a_j to get r_{ij} , then the comparison between element a_i and a_j yields a judgment that $r_{ij} = 1 - r_{ij}$

(5) Calculate the weight vector. Using the method of fuzzy mathematics, the judgement matrix is converted into a fuzzy judgement matrix, and the weight vector for each level is calculated. Determine the weights of matrix **R** using the weight calculation formula $W = \frac{1}{n} - \frac{1}{2a} + \frac{1}{an} \bullet \sum_{j=1}^{n} r_{ij}$, then multiply the weights of first- and second-tier indicators separately, and aggregate them level by level to finally get a comprehensive weight.

4.2.2. CRITIC Method

The CRITIC method provides a comprehensive assessment of the objective weighting of indicators, considering both the comparative strength among the evaluation indicators and the conflict they exhibit. The CRITIC method factors in both the variability of the indicators and the correlations between them; the greater the variability and the more significant the correlations, the higher the importance assigned. This approach exclusively relies on the inherent attributes of the data for scientific evaluation purposes.

Comparative strength pertains to the extent of value variation among evaluation programs for a given indicator, quantified by the standard deviation. A larger standard deviation signifies greater fluctuation, indicating a wider disparity in values among programs, which in turn results in a higher weighting.

The conflict or interplay between indicators is represented by the correlation coefficient; if there is a strong positive relationship between two indicators, the less they conflict, the lower the weight will be.

In the context of the CRITIC method, when the standard deviation remains certain, lesser conflict or correlation between indicators results in a smaller weight being assigned to them; the greater the conflict or correlation between indicators, the greater the weight given to them; furthermore, as the positive correlation between the two indicators intensifies (approaching a correlation coefficient of 1), the conflict diminishes, suggesting a higher degree of similarity in the information they provide when assessing the strengths and weaknesses of the programme.

The steps of the CRITIC method are as follows:

(1) Normalization of indicators. To mitigate the impact of different scales on evaluation outcomes, it is crucial to conduct a dimensionless processing of the indicators. The CRITIC weighting method typically employs either positive or negative scaling, and standard deviation is not

recommended due to it results in all standard deviations becoming unity, i.e. when the standard deviation of all the indicators is identical, the volatility indicator being meaningless. According to the correlation between the indicators and the security of the edge intelligent control platform, it can be seen that the selected indicators are positive indicators, i.e., the values of these indicators increase positively when the security level of the edge intelligent control platform is higher. It is processed to be positively oriented:

$$x'_{ij} = \frac{x_j - x_{\min}}{x_{\max} - x_{\min}} \tag{12}$$

Where x_j represents the original value, x'_{ij} denotes the processed value, and $x_{\max}$ and $x_{\min}$ correspond to the highest and lowest values among the indicators, respectively.

(2) Analyse the variability and conflict of indicators. Measure the standard deviation δ for each indicator and use correlation analysis to analyse the conflict between two indicators. The quantitative formula for conflictability is:

$$R_j = \sum_{i=1}^{m} (1 - r_{ij}) \tag{13}$$

Where r_{ij} represents the correlation coefficient between evaluation indicators i and j; and m denotes the total number of evaluation indicators.

(3) Calculate the objective weights of the indicators. Assess the information content for each indicator and derive the impartial weight W_{cj} for each. The calculation formula is:

$$C_j = R_j \times \delta_j \tag{14}$$

$$W_{cj} = \frac{c_j}{\sum_{i=1}^{m} c_j} \tag{15}$$

4.2.3. Integrated Empowerment

Determine the weights of the indicator combinations through the combination assignment method. Through the combination assignment method, the subjective weight W_{aj} obtained from the fuzzy hierarchical analysis method and the objective weight W_{cj} obtained from the CRITIC method are combined to calculate the combination weight, which improves the reasonableness of the result. The formula for calculating the combination weight w_j is:

$$w_j = \frac{W_{aj} \times W_{cj}}{\sum_{i=1}^{p} W_{aj} \times W_{cj}} \tag{16}$$

The fused weights are applied to the leaf nodes of the attack tree model, and the risk assessment for each node is determined by combining the benefit function and occurrence probability of the attack defence strategy of each node. The risk value of the root node can be solved according to the 'and' 'or' connection relationship in the attack tree, and the overall risk level is determined by the proportion of the risk value of the root node to the risk value of the entire edge intelligent control platform.

5. Conclusions and Future Work

Driven by the Internet of Things (IoT) and 5G technologies, risk assessment of edge intelligent control platforms has become a research topic that cannot be ignored. The risk assessment method based on hybrid game theory proposed in this paper is an important supplement to the existing suite of security risk assessment instruments. Through in-depth theoretical analysis and model construction, this study successfully applies hybrid game theory to the risk assessment of edge intelligent control platforms, providing a new theoretical tool and analytical framework for understanding and predicting the dynamic game between attackers and defenders.

The two-dimensional security risk assessment framework constructed in this paper not only covers the information and physical domains but also meticulously depicts the potential attack paths through the attack tree model, making the risk assessment more comprehensive and in-depth. In addition, by defining the benefit functions for both the attacker and the defender, and solving the Nash equilibrium point, this study can predict the probability of occurrence of attacks under different defence strategies, which provides scientific decision support for the selection of defence strategies.

Although the theoretical models and methods in this study are conceptually sound, they may encounter many challenges in practical applications. The focus of future endeavors will be on the following aspects: firstly, further optimization of the model to improve its applicability and flexibility in different application scenarios; secondly, exploring the integration of AI and machine learning techniques with risk assessment models to achieve smarter security management; and finally, the integration with real security scenarios will be strengthened, and the theoretical model will be validated and improved through collaboration with industry partners.

Acknowledgement: This study was supported by the National Key Research and Development Project of China (Project No. 2022YFB3104300).

References

1. Cai hu, D.Y. Application of ECC in Civil Aviation Rapid Transit System Based on “Cloud-Edge-End” Architecture. Automation Panorama, 2022, 39(12):26-29., J.; Z
2. Ding, C.T.; Cao, J.N.; Yang, L.; Wang, S.G. Edge Computing Overview: Applications, Status and Challenges. ZTE Technology Journal, 2019,25(3):2-7.
3. Bai, Y.Y.; Huang, Y.H.; Chen, S.Y.; Zhang, j.; Li, B.Q.; Wang, F.Y. Cloud Edge Intelligence: Edge Computing Methods for Power System Operation and Control and Their Application Status and Prospects. ACTA Automatica Sinica, 2020, 46(3): 397–410.
4. An, X.S.; Cao, G.X.; Mia, L.; Ren, S.B.; Lin, F.H. Intelligent Edge Computing Security Overview. Telecommunications Science, 2018, 34(7): 135-147.
5. Bourechak, A.; Zedadra, O.; Kouahla, M.N.; Guerrieri, A.; Seridi, H.; Fortino, G. At the Confluence of Artificial Intelligence and Edge Computing in IoT-Based Applications: A Review and New Perspectives. Sensors 2023, 23, 1639.
6. Y. Liu, M. Peng, G. Shou, Y. Chen and S. Chen, "Toward Edge Intelligence: Multiaccess Edge Computing for 5G and Internet of Things," in IEEE Internet of Things Journal, vol. 7, no. 8, pp. 6722-6747, Aug. 2020.
7. Y. Sahni, J. Cao, S. Zhang and L. Yang, "Edge Mesh: A New Paradigm to Enable Distributed Intelligence in Internet of Things," in IEEE Access, vol. 5, pp. 16441-16458, 2017.
8. W. Shi, J. Cao, Q. Zhang, Y. Li and L. Xu, "Edge Computing: Vision and Challenges," in IEEE Internet of Things Journal, vol. 3, no. 5, pp. 637-646, Oct. 2016.
9. M. W. Condry and C. B. Nelson, "Using Smart Edge IoT Devices for Safer, Rapid Response With Industry IoT Control Operations," in Proceedings of the IEEE, vol. 104, no. 5, pp. 938-946, May 2016.
10. Tripathy, S.S.; Imoize, A.L.; Rath, M.; Tripathy, N.; Bebortta, S.; Lee, C.-C.; Chen, T.-Y.; Ojo, S.; Isabona, J.; Pani, S.K. A Novel Edge-Computing-Based Framework for an Intelligent Smart Healthcare System in Smart Cities. Sustainability 2023, 15, 735.
11. V. Hayyolalam, M. Aloqaily, Ö. Özkasap and M. Guizani, "Edge Intelligence for Empowering IoT-Based Healthcare Systems," in IEEE Wireless Communications, vol. 28, no. 3, pp. 6-14, June 2021.
12. Shaik, T., Tao, X., Higgins, N., Li, L., Gururajan, R., Zhou, X., & Acharya, U. R. (2023). Remote patient monitoring using artificial intelligence: Current state, applications, and challenges. WIREs Data Mining and Knowledge Discovery, 13(2), e1485.
13. Saponara, S.; Donati, M.; Fanucci, L.; Celli, A. An Embedded Sensing and Communication Platform, and a Healthcare Model for Remote Monitoring of Chronic Diseases. Electronics 2016, 5, 47.

14. Chen, Y., et al. (2018). An Industrial Robot System Based on Edge Computing: An Early Experience. USENIX Workshop on Hot Topics in Edge Computing.
15. D. Kwon, M. R. Hodkiewicz, J. Fan, T. Shibutani and M. G. Pecht, "IoT-Based Prognostics and Systems Health Management for Industrial Applications," in IEEE Access, vol. 4, pp. 3659-3670, 2016.
16. F. Foukalas and A. Tziouvaras, "Edge Artificial Intelligence for Industrial Internet of Things Applications: An Industrial Edge Intelligence Solution," in IEEE Industrial Electronics Magazine, vol. 15, no. 2, pp. 28-36, June 2021.
17. Shi, W.S.; Sun, H.; Cao, J. Edge Computing: A New Computing Model for the Internet of Everything Era. Journal of Computer Research and Development, 2017,54(05):907-924.
18. Xing, Z.Q.; Cui, Y.H.; LV, X.D. Edge Node Platform Architecture for IoT. Computer Systems and Applications, 2022,31(05):85-93.
19. Guo, H.; He, X.Y.; Sun, X.J.; Chen, H.S.; Liu, Z.B.; Jie, J. Research on Security Risk Assessment of Edge Computing Applications for the State Grid. Computer Engineering and Science, 2020, 42(09): 1563-1571.
20. Zhou, X.R. Game Modeling and Vulnerability Analysis Strategies for Risk Assessment of Industrial Information Physical Systems.Southern Yangtze University, 2024.
21. Li Z, Wang P, Wang Z, et al. Flowgananomaly: Flow-based anomaly network intrusion detection with adversarial learning[J]. Chinese Journal of Electronics, 2024, 33(1): 58-71.
22. Wang Z X, Li Z Y, Fu M Y, et al. Network traffic classification based on federated semi-supervised learning[J]. Journal of Systems Architecture, 2024, 149: 103091.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.