The Value and Significance of the Security Evaluation Model for Information Systems in Edge Computing

Yanzheng Li[a]
Software College, Henan University, Kaifeng City, Henan Province, China

Keywords: Edge Computing, Security Evaluation, Evaluation Metrics, Model Improvement.

Abstract: With the advancement of technology, edge computing—a novel technology for data processing at the edge—has increasingly integrated with fields such as fifth-generation mobile communication (5G), the Internet of Things (IoT), and the Internet of Vehicles (IoV). However, due to the decentralized nature of edge architectures, terminal nodes are more susceptible to exposure in resource-constrained and low-trust complex network environments. Existing security evaluation standards and models for edge information systems still face shortcomings in terms of comprehensiveness, scientific rigor, and efficiency. Addressing these issues, the study of security evaluation models for edge computing information systems holds significant importance. First, traditional evaluation methods perform poorly in scenarios with limited data and non-strict normal distributions, highlighting the need for high-accuracy security evaluation models. Second, edge computing operates under resource constraints, and traditional fuzzy evaluation models require optimization in terms of resource consumption and adaptability, necessitating the development of efficient security evaluation models. Lastly, the dynamic characteristics of edge systems demand the construction of security evaluation models capable of adapting to rapid changes in network topology while ensuring the consistency and scientific validity of security evaluation benchmarks. This paper explores strategies for improving security assessment models for edge computing information systems and provides an overview of common methods, detection indicators, and existing achievements. Future efforts should focus on improving and optimizing edge information security evaluation models by integrating existing standards and protection frameworks to meet the demands of high accuracy, high efficiency, and dynamic adaptability.

1 INTRODUCTION

With the continuous advancement of technology, the rapid development of communication technologies, and the increasing prevalence of smart devices, a data processing technology based on edge-side operations—edge computing—has emerged. This technology has shown a growing trend of integration with fields such as fifth-generation mobile communication (5G), the Internet of Things (IoT), and the Internet of Vehicles (IoV) (Liu, Peng, Shou, et al., 2020). However, due to the decentralized design of edge architectures, the expanding range of application scenarios is accompanied by the risk of terminal nodes being more easily exposed to resource-constrained and low-trust complex network environments.

As edge computing is a relatively recent development, dedicated security evaluation standards for edge information systems remain scarce. Most existing security architectures and evaluation models for edge information systems are designed to address specific requirements, often lacking a holistic perspective. In terms of security indicator selection, the primary objectives have been to enhance scientific rigor and eliminate redundant information, with limited attention given to optimizing efficiency. The study of security evaluation models for edge computing information systems is therefore of great significance, as highlighted by the following three aspects:

First, edge information systems require high accuracy in security evaluation. Traditional single-weight assignment and first-order grey clustering methods have shown poor performance in edge scenarios characterized by limited data scale and non-strict normal distributions. Under such conditions, the original security evaluation data is prone to

[a] https://orcid.org/0009-0002-4009-8551

Li, Y.
The Value and Significance of the Security Evaluation Model for Information Systems in Edge Computing.
DOI: 10.5220/0013677700004670

In *Proceedings of the 2nd International Conference on Data Science and Engineering (ICDSE 2025)*, pages 33-39
ISBN: 978-989-758-765-8

fluctuations and discrepancies, and single-weight assignment methods are easily influenced by subjective factors or extreme data, thereby compromising the accuracy of system evaluation results. Consequently, it is necessary to adapt and improve these methods to develop high-accuracy models (Yuan et al., 2022).

Second, edge information systems are constrained by limited resources. Traditional fuzzy evaluation models still have significant optimization potential in terms of resource consumption. Additionally, the adaptability of traditional models in scenarios with limited data must be addressed. This necessitates the development of efficient security evaluation models that reduce computational demands while maintaining accuracy (Sun & Yu, 2019).

Finally, the spatiotemporal states of nodes in edge information systems may change rapidly, resulting in significant fluctuations in network topology and status. Thus, it is essential to build dynamic security evaluation models that extend beyond static models to accommodate dynamic scenarios and meet the demands of adaptive evaluation. Simultaneously, these models must ensure the consistency of security evaluation benchmarks to maintain the scientific rigor of dynamic system security evaluations (Wang & Xi, 2023).

In summary, existing research outcomes fall short of addressing the demands for high accuracy, high efficiency, and dynamic evaluation in edge information systems. It is imperative to adapt and refine the current edge information security evaluation models based on existing standards for information system security, edge computing security, and edge computing protection architectures to meet these requirements effectively.

2 MAINSTREAM METHODS FOR SECURITY EVALUATION MODELS OF EDGE COMPUTING INFORMATION SYSTEMS

2.1 Analytic Hierarchy Process (AHP)

The Analytic Hierarchy Process (AHP) is a multi-level, multi-criteria decision-making method with significant applications in system security evaluation. Its fundamental steps involve constructing a hierarchical structure for security evaluation, which typically divides the security assessment into three levels: the goal layer, the criterion layer, and the indicator layer.

The goal layer represents the overall security of the system, while the criterion layer is subdivided into several core domains, such as data security, network security, and device security. Each criterion layer contains multiple relevant indicators. For instance, the data security criterion may include indicators such as data integrity, access control, and encryption techniques. The network security criterion may encompass network traffic encryption, firewalls, and other measures, while device security pertains to hardware security, device protection, and related aspects.

Based on this structure, experts assign weights to each indicator using a scoring method. Experts leverage their practical experience and understanding of various aspects of security, along with the system's actual conditions, to evaluate the importance of each security indicator and assign corresponding weights. This process reflects both professional knowledge and ensures the rationality and scientific validity of the evaluation.

Subsequently, the weighted sum method is used to compute the comprehensive scores for each criterion layer and the goal layer. This involves multiplying each indicator's score by its corresponding weight and summing the results. Finally, the overall security evaluation of the system is obtained by analysing the comprehensive scores.

The advantages of AHP lie in its clear structure, ease of understanding, and ability to effectively integrate experts' subjective judgments. These features make it well-suited for security analysis and decision-making support in complex systems.

2.2 Fuzzy Comprehensive Evaluation Method

The fuzzy comprehensive evaluation method, based on fuzzy mathematics, is designed to handle uncertainty and ambiguity in complex systems, making it particularly valuable for system security evaluation (Yi, Cao, & Song, 2020).

The process begins with establishing an evaluation indicator set, which serves as the foundation for fuzzy comprehensive evaluation. For instance, when assessing data security, indicators might include data encryption, secure data transmission, and storage security. For network security, indicators could encompass network access control, traffic monitoring, and intrusion detection. Each indicator represents a specific aspect of the system's security, and a comprehensive evaluation of these indicators provides an overall understanding of the system's security status.

The next critical step is determining the evaluation grades. Security levels are typically categorized into grades such as "Very Secure," "Relatively Secure," "Average," and "Risky," with clear standards defined for each level. In practice, these security grades are not strictly defined but are represented using fuzzy membership degrees.

Subsequently, a fuzzy matrix is constructed. This involves assigning membership degrees for each indicator under different security grades based on actual conditions or expert opinions. These membership degrees reflect the extent to which an indicator conforms to a particular security grade, thereby forming the basis for comprehensive evaluation.

Finally, the overall security membership degree of the system is calculated using membership functions and weighted computations. This process combines the weights of individual indicators to produce a comprehensive evaluation result.

This method not only accommodates uncertainty factors but also provides a more flexible and objective security evaluation under various conditions, making it a robust approach for analyzing complex systems.

2.3 PageRank-Based Weighting Method

The PageRank-based weighting method leverages the principles of the PageRank algorithm to determine indicator weights (Langville & Meyer, 2006).

First, an indicator correlation network is constructed, where each indicator is treated as a node within the network. The relationships between indicators are determined by calculating their correlation or similarity, forming connections between nodes.

Next, the PageRank algorithm is applied to iteratively compute the weight of each indicator based on the connections within the network. The algorithm posits that an indicator's weight is influenced not only by its inherent properties but also by other indicators pointing to it. Indicators of higher importance pointing to a particular indicator will enhance its weight.

Through iterative computation, the algorithm eventually converges, yielding the final weight for each indicator, which represents its importance in the overall evaluation.

This method objectively assigns weights to indicators by fully accounting for their interrelationships through an automated process. As a result, it produces more scientific and comprehensive evaluation outcomes.

2.4 Entropy Weighting Method

The entropy weighting method determines weights based on the amount of information provided by each indicator, where entropy is used as a measure of the information conveyed by uncertain events and reflects the degree of variability among indicators.

Specifically, for the security evaluation indicators of an edge information system, greater variation in the raw data of a particular indicator indicates higher volatility and divergence in its assessments. This implies that the indicator provides more information and has a greater impact on the evaluation results, warranting a higher weight. Conversely, if an indicator’s raw data shows minimal variation, it contains less information and has a lower impact on the final evaluation, justifying a lower weight (Luo, Chen, & Lu, 2020).

By quantifying the variability of each indicator, the entropy weighting method ensures that weights are assigned objectively, reflecting the contribution of each indicator to the overall evaluation.

2.5 Principal Component Analysis

Principal Component Analysis (PCA) is a classical dimensionality reduction technique widely used in fields like data analysis, pattern recognition, and statistics. Its core principle is to transform high-dimensional data into a lower-dimensional space through linear transformation while preserving as much of the original information as possible. The process involves standardizing the data to remove the influence of different variable scales, calculating the covariance matrix to analyze linear relationships, and performing eigenvalue decomposition or singular value decomposition to derive principal components. By selecting components with high cumulative variance contribution, PCA effectively reduces dimensions, minimizes data redundancy, and improves computational efficiency and model generalization.

3 EVALUATION STANDARDS FOR SECURITY ASSESSMENT MODELS IN EDGE COMPUTING INFORMATION SYSTEMS

3.1 Indicators for Determining Model Accuracy

3.1.1 The first-to-last consistency rate

The first-to-last consistency rate is a metric for evaluating the consistency of a system when processing time-series data or multi-stage tasks. It measures the alignment between the initial input in the first stage and the output in the final stage. Calculated as (Number of Consistent Samples / Total Samples) × 100%, consistent samples are those where the initial and final states or features match. A high consistency rate reflects stable performance, strong resistance to interference, and good continuity in information processing, making it an important standard for ensuring system security (Cheng, 2018).

3.1.2 maximum membership degree

The maximum membership degree is a principle in fuzzy mathematics used to determine an element's affiliation with a fuzzy set. It indicates that when an element's membership degree is the highest within a set, it is most likely to belong to that set. With values ranging from 0 to 1, a membership degree closer to 1 signifies stronger affiliation. This principle is widely used in fuzzy classification and reasoning. For instance, in edge computing security assessments, the maximum membership degree can help determine whether a behaviour is "normal" or "abnormal," supporting security decisions (Guo, 2024).

3.2 Indicators for Determining Model Efficiency

3.2.1 Fuzzy Evaluation Deviation

Fuzzy evaluation deviation is an indicator used to measure the degree of deviation between a system's evaluation results and its ideal target. It is widely applied in multi-attribute decision-making and fuzzy comprehensive evaluation. By constructing an evaluation index system and membership functions, the deviation is calculated as the distance between the actual evaluation results and the ideal optimal or worst states, quantifying the degree of deviation. A smaller deviation indicates that the evaluation results are closer to the ideal state, while a larger deviation signifies a significant gap between system performance and the target. This indicator helps identify weaknesses in the system and provides a basis for optimization.

3.2.2 Average Information Quantity

The variation in average information quantity is used to reflect the effectiveness of indicator selection. A value exceeding 100% indicates that the average amount of information has increased after the selection compared to before, suggesting that the selection process had a positive impact.

3.2.3 Average Information Contribution Variation

The average information contribution variation reflects the information content of the indicator set after selection. A higher value indicates stronger representativeness of the indicator set.

3.3 Indicators for Determining Model Dynamism

Relative closeness is an indicator used to measure the consistency of results from different selection methods in security evaluations. It assesses the effectiveness and reliability of these methods by comparing their results with a benchmark value. Deviation is determined by calculating the differences between the evaluation results of various methods and the benchmark value, often measured using statistical methods such as standard deviation or variance. By utilizing the deviation of relative closeness, the validity of a security evaluation model can be verified. If the results from different methods show small deviations, it indicates that the model has high accuracy and stability. Conversely, larger deviations suggest that the model requires adjustments or optimization (Guo, 2024).

4 CURRENT STATE OF SECURITY EVALUATION MODELS FOR EDGE COMPUTING INFORMATION SYSTEMS

4.1 Accuracy Improvements

To meet the high-accuracy requirements of information system security evaluation in edge computing scenarios and enhance the scientific rigor of weight calculation methods, Guo proposed an adaptation of the single-weight first-order grey clustering security evaluation model. This adaptation introduces a high-accuracy security evaluation grading model based on a combination of subjective and objective weighting and second-order grey clustering. The effectiveness of the improved model was analysed using two metrics: the membership difference coefficient and the consistency rate of the evaluation results. Experimental results demonstrate that the model performs well in terms of consistency rate, indicating coherent evaluation outcomes. Additionally, the model showed significant advantages in membership difference coefficient compared to the original, suggesting improved discrimination in membership values and, consequently, enhanced evaluation accuracy (Guo, 2024).

4.2 Efficiency Improvements

To address the resource constraints in edge computing and the challenges posed by non-prominent normal distribution patterns in original security evaluation data in edge-distributed scenarios, Guo proposed an efficient security evaluation model. This model is based on Spearman PCA and differentiation-driven indicator screening and incorporates three measurement metrics: the Average Information Quantity Change Degree (AQICD), Average Information Contribution Change Degree (AICCD), and Fuzzy Evaluation Deviation. Experimental results show that compared to traditional models without indicator screening, the proposed model reduces resource consumption to approximately one-third while limiting the evaluation result deviation caused by indicator screening to only about 1.8%. This demonstrates a favourable balance between energy efficiency and performance (Guo, 2024).

4.3 Dynamic Improvements

To address the dynamic security evaluation needs of edge information systems, particularly in the context of Internet of Vehicles (IoV), Guo focused on solving dynamic security evaluation challenges in resource-constrained scenarios while optimizing model efficiency and ensuring accuracy. Guo developed a dynamic security evaluation model based on time-varying, adaptive screening of intra-class indicator effectiveness. The model improves the traditional GFRS method by applying the grey F-statistical association method for clustering, and then using intra-class indicator effectiveness to perform time-varying adaptive screening of both subjective and objective indicators. This results in the GFCIV indicator screening method, which enhances the overall operational efficiency of the security evaluation model. Compared to the GFRS-CGTOPSIS model that uses traditional GFRS methods for indicator screening, the proposed model exhibits more reasonable distribution of indicator weights, lower evaluation result deviation, and reduced resource consumption, making it more suitable for dynamic security evaluations in edge information systems (Guo, 2024).

5 DISCUSSION ON THE LIMITATIONS OF CURRENT RESEARCH METHODS AND COUNTERMEASURES

5.1 Some models perform poorly when there is significant divergence in subjective indicators, such as expert scoring.

5.1.1 Introduction of Conflict Coordination Mechanism

To address the issue where some models perform poorly when there is significant divergence in subjective indicators, such as expert scoring, a conflict coordination mechanism can be introduced for data preprocessing to improve the model's stability. First, statistical methods can be used to quantify the degree of divergence between experts, such as using the Kappa coefficient (κ) to measure the consistency of ratings or classifications. The formula for calculating the Kappa coefficient is $\kappa = (Po - Pe) / (1 - Pe)$, where Po represents the actual observed consistency and Pe represents the expected consistency based on random allocation. When κ = 1, it indicates perfect consistency; κ = 0 means consistency is due to chance; and when κ < 0, the consistency is lower than random levels (Cohen, 1960). Additionally, a divergence degree can be defined as an additional indicator to monitor the model's sensitivity to expert divergence. If the divergence degree exceeds a preset threshold, smaller weights can be assigned to experts with significant divergence, thereby reducing their impact on the model's results.

5.1.2 Introduction of Genetic Algorithm

To more efficiently find the global optimal solution for weight allocation and enhance the model's robustness, a genetic algorithm can be introduced to optimize expert score weight distribution. The genetic algorithm simulates the process of natural selection to search for the optimal combination of parameters, thus reasonably adjusting expert score weights when the divergence exceeds the threshold. Specifically, expert weights are designed as optimization variables (genes), and a fitness function is defined, where the evaluation criterion is the error between the weighted evaluation results and the true results. During the algorithm execution, the population is first initialized with a randomly generated initial weight set. Then, new candidate solutions are generated through crossover and mutation operations. Finally, the better solutions are selected based on fitness values and retained until the algorithm converges or reaches a predetermined number of generations (Holland, 1975). This approach allows dynamic adaptation to expert divergence and improves the model's ability to process subjective scoring data.

5.2 Some models' subjective indicators cannot dynamically change with the simulation process, which does not align with real-world situations.

To address the issue where certain models' subjective indicators cannot dynamically change with the simulation process, time series forecasting methods can be used to simulate the dynamic changes of these indicators, thus improving the alignment of simulation results with real-world environments. Time series forecasting predicts future trends based on historical data, reducing the burden of frequent data collection and expert involvement, while striving to realistically simulate the actual environment. For linear and stationary subjective indicators, the Auto-Regressive Integrated Moving Average (ARIMA) model can be used, as it captures short-term variations and trends, improving forecast accuracy by optimizing parameters p, d, and q (Box et al., 2015). For more complex nonlinear indicators, the LSTM (Long Short-Term Memory) model based on neural networks can be adopted. LSTM is particularly good at modelling long-term dependencies and nonlinear dynamic changes, making it suitable for handling long-term complex indicator variations, and it can optimize model performance by adjusting hyperparameters such as the number of neurons in hidden layers and learning rate (Hochreiter & Schmidhuber, 1997). In the simulation tests, ARIMA can be used to evaluate the model’s performance in stationary scenarios, while LSTM can simulate the nonlinear dynamic environment with randomness and sudden changes, providing a comprehensive assessment of the model's adaptability and robustness.

6 CONCLUSIONS

This paper reviews the current major research progress in the security evaluation of edge computing information systems, analysing and discussing aspects such as evaluation index design and method optimization. The research shows that combining statistical methods with intelligent algorithms can significantly improve the accuracy and efficiency of the evaluation. However, existing studies still have certain limitations in areas such as the stability of models influenced by indicators and the dynamic modelling of subjective indicators. Future research should focus on developing more efficient multimodal data processing algorithms and exploring adaptive weighting methods to balance the impact of divergences on results. In conclusion, the research on security evaluation of edge computing information systems not only has significant theoretical value but also has broad application prospects in the field of information security assurance.

REFERENCES

Box, G. E. P., Jenkins, G. M., Reinsel, G. C., & Ljung, G. M. 2015. Time series analysis: Forecasting and control (5th ed.). Wiley.

Cheng, R. 2018. Information security quality evaluation method for network security equipment (Doctoral dissertation). Beijing University of Posts and Telecommunications.

Cohen, J. 1960. A coefficient of agreement for nominal scales. Educational and Psychological Measurement, 20(1), 37–46.

Greenacre, M., Groenen, P. J. F., Hastie, T., et al. 2022. Principal component analysis. Nature Reviews Methods Primers, 2(1), 100.

Guo, Z. 2024. Research on information system security evaluation model for edge computing (Doctoral dissertation). Beijing University of Posts and Telecommunications.

Hochreiter, S., & Schmidhuber, J. 1997. Long short-term memory. Neural Computation, 9(8), 1735–1780.

Langville, A. N., & Meyer, C. D. 2006. Google's PageRank and beyond: The science of search engine rankings. Princeton University Press.

Liu, Y., Peng, M., Shou, G., et al. 2020. Toward edge intelligence: Multiaccess edge computing for SG and Internet of Things. IEEE Internet of Things Journal, 7(8), 6722–6747.

Luo, N., Chen, L. D., & Lu, S. B. 2020. Reliability evaluation of power distribution network operation based on cluster analysis and improved grey correlation. Journal of Wuhan University of Technology (Engineering Edition), 53(07), 636–642.

Sun, H., & Yu, Y. 2019. Public safety system for edge computing based on heterogeneous multi-source in natural environments. ZTE Technology, 25(3), 43-49.

Wang, Y., & Xi, J. 2023. Resource allocation strategy for vehicular edge computing task offloading with privacy protection. Computer Applications, 44(2), 372-378.

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

Yuan, J., Mao, H., & Wang, N. 2022. Dynamic service deployment strategy with resource constraints in mobile edge computing. Computer Applications, 1662-1667.