Terminal Security Configuration Optimization under Edge Computing

Qianru Wang, Aidong Xu, Yunan Zhang, Minggui Cao, Jianfang Song, Yixin Jiang and Hong Wen

1School of Aeronautics and Astronautics, University of Electronic Science and Technology of China (UESTC), Chengdu 611731, China
2Electric Power Research Institute, China Southern Power Grid Co., Ltd. Guangzhou, China
Email: wqr_uestc@163.com; sunlike@uestc.edu.cn
*Corresponding Author Email: 201821100211@std.uestc.edu.cn

Abstract. It is an important task of system security management to configure terminal security policy reasonably in edge computing (EC) to implement necessary security protection for terminals and EC system. Therefore, this paper analyses the security goals and requirements of terminal access for multi-service EC systems under the power grid, conducts terminal security risk assessment based on the AHP algorithm, and proposes an edge computing platform terminal security configuration optimization strategy, creatively using the OS-ELM algorithm. A framework for cloud training and edge-side online learning to meet the real-time and lightweight communication needs of edge platforms.

1. Introduction
With the continuous advancement of smart grid construction, the scale of the power system continues to expand [1], the number of smart terminals has increased sharply, and the power business also shows a trend of diversity and real-time, resulting in massive heterogeneous data ([2], [3]). Edge computing is at the edge of the network and close to the source of the data, and can provide nearby edge services, which can meet the needs of industry services such as real-time business, low transmission delay, and intelligent application. However, the introduction of this new service model will not only relieve the pressure of the smart grid system, but also bring more complex and diverse security issues [4]. The development of a comprehensive and flexible terminal security protection framework is to ensure that edge computing technology is used in the smart grid system. The key to smooth application. In fact, the specific application of edge computing is still in the development stage, and the corresponding terminal security research is very few. In reference [5], a quantitative edge computing side terminal security access strategy selection scheme is proposed, which can protect the terminal and data from security Risks and threats are quantified, appropriate algorithms are selected, and the edge computing-side terminal security access strategy selection is performed through quantified objective standards [6]. On this basis, this paper further summarizes the security assessment items applicable to the information security of smart grid edge computing, and constructs the national grid edge computing terminal information security assessment model based on the AHP algorithm, and designs the terminal security configuration strategy optimization model to make the terminal access time satisfy the security requirements of the business system while giving the right security protection [7].
2. Terminal Security Risk Analysis

2.1. Optimal Strategy of Power Terminal Security Configuration under Edge Computing
Terminal security configuration optimization includes four stages: risk assessment preparation, security vulnerability identification, risk analysis and security configuration, as shown in Figure 1.

The security risk assessment of the smart terminal refers to the loss and impact of the security breach caused by the lack or destruction of a certain security measure in the smart terminal security protection mechanism, which is the threat, system security vulnerability and the resulting Assessment of the magnitude and impact of risks [8].

2.2. Terminal Security Evaluation Information Collection
According to standards "GBT37138-2018 Electric Power Information System Security Level Protection Implementation Guide"，"GB/T 36047-2018 Electric Power Information System Security Inspection Specification"，a certain type of security mechanisms, such as data security mechanism，identity Authentication security mechanism，access control security mechanism，user security mechanism etc.，specific security evaluation item \( a_i \)，the administrator assigns a weight value of \( v_i \) to the check item based on whether the actual situation of the power system information security work on the edge platform system meets the check item description [9]，according to the inspection result, the quantified value \( p_i \) is assigned，as shown in Table 1. The quantified value of a certain type of safety mechanism check result is calculated by formula 1.

\[
r_t = \sum_{i=1}^{n} v_i p_i
\]

Among them, \( r_t (0 < r_t < 1) \) is the evaluation result of the current t-th security mechanism of the terminal, \( t = 1, 2, Kn \) and \( m \) is the total number of security mechanisms. The specific quantitative value of the evaluation item can be obtained through methods such as terminal evaluation tools or expert analysis. It is the weight of the i-th evaluation item, which can be obtained through the national electric power information security related standards or the expert experience method，\( i = 1, Kn \)，\( n \) is the total number of evaluation items of a certain evaluation category.

2.3. Terminal Security Risk Analysis Based on AHP Algorithm
The security risk assessment elements of smart terminals are mainly divided into three aspects: asset loss, threat and vulnerability [10].

(1) According to the analysis of the communication threat of the intelligent terminal of the electric power information system [11]，a risk assessment model can be established as shown in Figure 2. Through the AHP algorithm，the current system terminal security mechanism weight \( W = \{ \omega_1, \omega_2, \ldots, \omega_m \}，0 < \omega_m < 1 \) are calculated according to a scale of 1-9.
Figure 1. Edge-side terminal security management process.

Figure 2. Power terminal security risk assessment model.

(2) By using the evaluation tool or questionnaire survey method, the terminal security vulnerability evaluation matrix according to Eq. (1) can be obtained. Let $r_{kt}$ ($k = 1, \ldots, l, t = 1, \ldots, m$) be the score of the terminal $k$ on the $t$-th security mechanism, the risk score of each terminal on the access edge can be calculated by Eq. (2), and the overall security risk level of the terminal can be obtained by referring to Table 1.

$$V = R \times W^T = \begin{bmatrix} r_{11} & r_{12} & \cdots & r_{1m} \\ r_{21} & r_{22} & \cdots & r_{2m} \\ \mathbf{M} & \mathbf{O} & \mathbf{M} \\ r_{l1} & r_{l2} & \cdots & r_{lm} \end{bmatrix} \times \begin{bmatrix} \omega_1 \\ \omega_2 \\ \mathbf{M} \\ \omega_m \end{bmatrix}$$ (2)
Table 1. Terminal security mechanism evaluation form.

| Security Evaluation | Security check items | Weights | Quantized value |
|---------------------|----------------------|---------|----------------|
| Type t safety mechanism | Item i specific inspection content | \(v_i \left( \sum_{i=1}^{n} v_i = 1 \right)\) | Totally suitable \(p_i = 1\) |
|                      |                      |         | Partial match \(p_i = 0.5\) |
|                      |                      |         | Incompatible \(p_i = 0\) |

The \(t\)-th security mechanism risk score is obtained by formula 3, and the vulnerability risk level of each security mechanism of the terminal can be obtained by comparing with Table 2 [5].

\[ v_{ls} = \omega_l r_{ls} \]  

Table 2. Security Risk Assessment Level Table.

| Security risk level | Level I | Level II | Level III | Level IV |
|---------------------|---------|----------|-----------|----------|
| Terminal security risks | 0 ~ \(m/4\) | \(m/4 \sim m/2\) | \(m/4 \sim m/2\) | 3\(m/4 \sim m\) |
| Security mechanism risk | 0 ~ 0.25 | 0.25 ~ 0.5 | 0.5 ~ 0.75 | 0.75 ~ 1 |

3. Terminal Security Policy Configuration
In this paper, on the edge computing system platform, according to the terminal information system security requirements, the terminal access meets the security standards ([12], [13]). The information security manager collects the actual terminal security information, conducts the security mechanism vulnerability risk assessment on the platform, and considers the terminal computing resources and system communication delay requirements are optimized for security configuration, so that the terminal can meet the security requirements of the business system while providing proper security protection when accessing [14]. The security policy configuration steps are as follows:

1. To set the evaluation matrix of the \(t\)-th type of terminal security mechanism under the edge computing system, it is necessary to consider the required configuration strategy of the terminal from the three dimensions of the terminal's current security mechanism vulnerability risk, delay requirements and computing resources. Set the terminal type \(t\) safety mechanism evaluation matrix \(A\):

\[
A = \begin{pmatrix}
    a_1^1 & a_2^1 & a_3^1 \\
    a_1^2 & a_2^2 & a_3^2 \\
    M & O & M \\
    a_1^l & a_2^l & a_3^l
\end{pmatrix}
\]

Among them, \(a_k^i\) is the corresponding security mechanism risk level of terminal \(k\); \(a_i^k\) is the quantified value of terminal \(k\)'s current system or task delay requirement, which can be obtained from Table 3; \(a_3^k\) is the quantified value of terminal \(k\)'s computing resources, which can be obtained from Table 3. \(k = 1, \ldots, l\), \(l\) is the total number of access terminals on the edge computing platform.

2. The edge side obtains the security policy evaluation matrix \(B\) from the three dimensions of security strength, encryption efficiency, and resource consumption:
\[
B = \begin{pmatrix}
b_1^1 & b_1^2 & \cdots & b_1^p \\
b_2^1 & b_2^2 & \cdots & b_2^p \\
M & O & M \\
b_3^1 & b_3^2 & \cdots & b_3^p 
\end{pmatrix}
\]

Among them, \( b_j^i \) is the quantitative value of security strength of security policy \( j \), \( b_j^i \) is the quantitative value of encryption efficiency of security policy \( j \), \( b_j^i \) is the quantitative value of resource consumption of security policy \( j = 1, 2, \cdots, p \), \( p \) is the number of security policy types.

### Table 3. Index quantification table.

| Quantized value | 1 | 2 | 3 | 4 |
|-----------------|---|---|---|---|
| Risk level      | IV| III| II| I  |
| Delay requirements | Minutes | <6s | <3s | <1s |
| Computing resources | Weak | Strong |
| Security strength | Weak | Standard | Safe | Very safe |
| Encryption efficiency | Slow | Ordinary | Fast | Very fast |
| Encryption resource consumption | Very high | High | Ordinary | Low |

(3) The quantified value of security protection after adopting different security strategies for each terminal under a certain security mechanism is calculated:

\[
Z = A \cdot B = \begin{pmatrix}
z_1^1 & z_2^1 & \cdots & z_p^1 \\
z_1^2 & z_2^2 & \cdots & z_p^2 \\
M & O & M \\
z_1^1 & z_2^1 & \cdots & z_p^1 
\end{pmatrix}
\]

Among them, \( z_j^i \) is the quantified value of security protection for the \( i \)-th terminal after adopting the \( j \)-th security policy in a certain security mechanism, and the security protection policy corresponding to the maximum value of \( z_j^i \) is directly selected as the security configuration of each terminal to achieve the optimization effect.

### 4. Security Policy Configuration Model Based on OS-ELM Algorithm

Online Sequential ELM (Online Sequential ELM, OS-ELM) is an improved algorithm based on the traditional extreme learning machine. It has online sequential learning capabilities. It can use real-time data to learn and update output weights. The algorithm is more robust and generalized. Strong. Taking into account the complexity of the actual communication environment of the terminal in the power information system and the time-varying nature of the system, there are many variables in the evaluation items and security algorithms in the actual security policy configuration process [15], so the OS-ELM algorithm with good robustness is more capable of meeting the needs of the actual system.

The training steps and principles of the security policy configuration model based on the OS-ELM algorithm are as follows:

1. Determine the initial training sample set \( D_0 = \{ (x_i, y_i) \mid x_i \in R^k, y_i \in R^k \}, i = 1, \ldots, n_0 \), \( n_0 \) is the number of the first batch of terminal sample data. For the built simulation model, each batch of
samples is a sample set composed of randomly selected terminal test item data and security policy data after preprocessing;

(2) The connection weight matrix $W$ between the input layer and the hidden layer and the bias matrix $B$ of the hidden layer nodes are generated by random generation;

(3) Determine the initial output weight matrix $\beta^{(0)}$.

(4) After the edge platform collects a new sample set $D_i = \{(x_i, y_i) | x_i \in \mathbb{R}^p, y_i \in \mathbb{R}^q, p = p_0 + 1, \ldots, q, p = n_0 + 1, q = n_0 + n_i\}$, it can be uploaded to the cloud server. $n_i$ represents the number of data in the new batch of samples.

(5) The new output weight can be calculated according to the known parameters, so that the output weight matrix can be updated according to the training results of $n_1$ samples in the newly input sample set. With the model built by OS-ELM, the cloud online learning process does not need to scan historical sample data, saving a lot of training time, training speed is greatly improved, and the model on the edge platform can not interrupt the model use process.

5. Conclusions
This article discusses terminal security under edge computing, and proposes an edge-side terminal security configuration optimization strategy, which can achieve a comprehensive assessment of security performance and complexity through the quantitative relationship between the edge computing device security policy and the risk of the terminal or data application. The most resource saving and the greatest optimization of the security performance of the edge computing system to meet the security requirements.

6. Acknowledgments
This work is supported by the National major R & D program (No. 2018YFB0904900, 2018YFB0904905).

7. References
[1] H. Wen, P. Ho, C. Qi and G. Gong, "Physical layer assisted authentication for distributed ad hoc wireless sensor networks," *IET Information Security*, vol. 4, no. 4, pp. 390-396, December 2010.
[2] H. Wen, P. Ho and B. Wu, "Achieving Secure Communications over Wiretap Channels via Security Codes from Resilient Functions," *IEEE Wireless Communications Letters*, vol. 3, no. 3, pp. 273-276, June 2014.
[3] S. Chen et al., "Internet of Things Based Smart Grids Supported by Intelligent Edge Computing," *IEEE Access*, vol. 7, pp. 74089-74102, 2019.
[4] B. Ji, Y. Li, B. Zhou, C. Li, K. Song and H. Wen, "Performance Analysis of UAV Relay Assisted IoT Communication Network Enhanced With Energy Harvesting," *IEEE Access*, vol. 7, pp. 38738-38747, 2019.
[5] Aidong Xu, Qianru Wang, Yixin Jiang, Runfa Liao, Yunan Zhang, Yi Chen, Hong Wen, Jinran Du, "Quantitative selection of secure access policies for edge computing side terminals," *2019 International Conference on Information, Communication Technology and Automation*, pp. 68-73.
[6] F. Xie et al., "Optimized Coherent Integration-Based Radio Frequency Fingerprinting in Internet of Things," *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3967-3977, Oct. 2018.
[7] H. Wen et al., "A Cross-Layer Secure Communication Model Based on Discrete Fractional Fourier Fransform (DFRFT)," *IEEE Transactions on Emerging Topics in Computing*, vol. 3, no. 1, pp. 119-126, March 2015.
[8] H. Wen, Y. Wang, X. Zhu, J. Li and L. Zhou, "Physical layer assist authentication technique for smart meter system," *IET Communications*, vol. 7, no. 3, pp. 189-197, 12 February 2013.
[9] Y. Xie, H. Wen, B. Wu, Y. Jiang and J. Meng, "A Modified Hierarchical Attribute-Based Encryption Access Control Method for Mobile Cloud Computing," *IEEE Transactions on Cloud Computing*, vol. 7, no. 2, pp. 383-391, 1 April-June 2019.
[10] L. Hu, H. Wen, B. Wu, J. Tang and F. Pan, "Adaptive Base Station Cooperation for Physical Layer Security in Two-Cell Wireless Networks," *IEEE Access*, vol. 4, pp. 5607-5623, 2016.

[11] L. Hu et al., "Cooperative Jamming for Physical Layer Security Enhancement in Internet of Things," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 219-228, Feb. 2018.

[12] S. Chen et al., "A Novel Terminal Security Access Method Based on Edge Computing for IoT," *International Conference on Networking and Network Applications (NaNA)*, Xi’an, China, 2018, pp. 394-398.

[13] Q. Li et al., "A Risk Assessment Method of Smart Grid in Cloud Computing Environment Based on Game Theory," *IEEE 5th International Conference on Cloud Computing and Big Data Analytics (ICCCBDA)*, Chengdu, China, 2020, pp. 67-72.

[14] H. Zhang, Q. Li, Y. Qi, J. Hou and Y. Liu, "The Research Reviewed of Edge Network Active Safety Defense Technology," *IEEE Fifth International Conference on Big Data Computing Service and Applications (BigDataService)*, Newark, CA, USA, 2019, pp. 242-246.

[15] M. Luo, H. Ma, X. Wang and X. Zhang, "PICO and OS-ELM-LRF Based Online Learning System for Object Detection," *IEEE International Conference on Mechatronics and Automation (ICMA)*, Tianjin, China, 2019, pp. 1548-1553.