Computing, Performance and Communication Systems (2025)
Clausius Scientific Press, Canada
DOI: 10.23977/cpcs.2025.090115
ISSN 2371-8889 Vol. 9 Num. 1

Research on Power Information Security Protection and Big Data Privacy Protection in Internet Communication

Yong Fu

Beijing Remarkables United Technology Co., Ltd., Beijing, 100192, China

Keywords: Power Information Security; Privacy Protection; Internet Communication; Big Data

Abstract: This paper conducts a systematic study on the multimedia communication security and big data privacy protection problems faced during the Internet-based transformation of power systems. It analyzes the unique systematic security risks, new attack surfaces, and privacy protection requirements in the power Internet communication environment, and constructs a "proactive defense-privacy enhancement" dual-drive technology system. On the security protection level, it proposes a data encryption transmission scheme based on domestic cryptographic algorithms, a zero-trust dynamic access control mechanism, a multimedia steganography detection method, and a collaborative emergency response system. On the privacy protection level, it innovatively adopts dynamic anonymization and differential privacy fusion technology, a federated learning framework, and a full lifecycle security management system. Empirical application through a provincial power company shows that the system can reduce the incidence of security events by more than 75% and achieve privacy control while ensuring business real-time performance. The research provides a systematic solution for building a secure and reliable power Internet communication environment, and has important practical value for promoting the construction of a new type of power system.

1. Introduction

With the deepening integration of the Energy Internet and digital transformation, the operational mode of power systems is undergoing profound changes. Internet communication technologies, especially multimedia communication (such as video surveillance, remote inspection, and audio dispatch), has deeply penetrated core links including power generation, transmission, transformation, and distribution, becoming a key carrier supporting the reliable operation of smart grids [1, 2]. However, the openness of communication technology and business integration, while improving operational efficiency and intelligent levels, has also greatly expanded the system's attack surface, making critical power information infrastructure face unprecedented information security and data privacy challenges. Traditional static security models based on boundary protection are difficult to cope with the new Internet communication environment characterized by heterogeneous equipment, complex links, and high real-time data requirements. Building an active and intrinsic security protection system adapted to it has become an urgent need for industry development.

Currently, although research on power information security has made significant progress, it is mostly focused on traditional industrial control network boundary protection or the detection of a single type of attack. In the face of advanced persistent threats (APTs), data theft based on steganography, and privacy leakage risks caused by the aggregation of massive user and device data, existing research still has shortcomings in multimedia communication security, continuous protection during data flow, and the dynamic balance between privacy and effectiveness[3]. Especially in the context of power big data, there is an inherent contradiction between data value and privacy protection: over-protection may lead to the destruction of data value, affecting real-time grid control and user services; insufficient protection is prone to major security incidents and compliance risks.

This research aims to systematically study the new information security and privacy protection issues faced by power systems in the Internet communication environment, breaking through the limitations of traditional security architectures. The research focuses on building a defense-in-depth system that integrates active defense and privacy-enhancing technologies (PETs), focusing on solving the confidentiality and integrity of multimedia data during transmission and storage, as well as the privacy control of multi-source heterogeneous data in integrated utilization. The paper will start by analyzing the unique security challenges of power Internet communication, and respectively elaborate on the active protection technology path for network attacks and the protection computing scheme for data privacy, and finally provide theoretical support and practical reference for building a secure, reliable, and compliant new power system communication infrastructure.

2. Challenges and Characteristics Analysis

2.1 Systemic Risks

As critical national information infrastructure, the power system faces unique and systemic information security risks that differ from traditional IT systems. A large number of production control devices within the power system are designed based on traditional industrial control protocols and dedicated hardware, resulting in inherent defects such as long vulnerability patching cycles and difficult security updates. These devices generally lack intrinsic security mechanisms, creating a large number of attack entry points that are difficult to eliminate quickly. Advanced Persistent Threats (APTs) targeting power systems exhibit highly customized characteristics. Attackers evade traditional security detection mechanisms through long-term lurking and slow infiltration. A more harmful threat lies in the precise tampering of measurement data, status information, or scheduling instructions. Such attacks do not immediately trigger system failures, but rather mislead the control system into making incorrect decisions by injecting subtle deviations, which may ultimately lead to cascading failures and widespread power outages[4]. This systemic risk characteristic indicates that power information security has shifted from single-point protection to the need to build a comprehensive and multi-layered defense-in-depth system.

2.2 Vulnerability Analysis

The introduction of internet communication protocols has significantly expanded the attack surface of power systems. The widespread application of TCP/IP protocols has broken the physical isolation environment of traditional power industrial control systems, exposing the system to more threats from public networks. The large-scale access of Internet of Things devices such as video surveillance, smart sensors, and inspection drones improves system intelligence while also introducing new vulnerabilities such as insufficient device identity authentication strength and weak communication channel protection[5]. Authentication mechanisms based on static passwords cannot

effectively prevent credential theft and man-in-the-middle attacks, while multimedia communication data often lacks end-to-end encryption protection during transmission, making it extremely vulnerable to eavesdropping or tampering. Of greater concern is that attackers can utilize the data redundancy characteristics of multimedia files to conceal malicious code or stolen data within normal business data through steganography, and exfiltrate it. This advanced threat method can effectively evade the detection of traditional security equipment, posing a serious threat to the confidentiality of power dispatch data.

2.3 Demands and Contradictions

Privacy protection in the context of power big data faces the core contradiction between value utilization and privacy risks. High-frequency electricity consumption data collected by smart meters can accurately reflect users' lifestyles, habits, and even the composition of their electrical equipment, making it extremely privacy-sensitive. Equipment condition monitoring data is not only used for fault prediction but may also be used to infer trade secrets such as production processes and equipment layouts. Dispatch instruction data is directly related to the real-time balance and safe operation of the power grid, requiring the highest level of confidentiality. These data specificities require privacy protection solutions to go beyond traditional static de-identification and access control, necessitating the establishment of dynamic, fine-grained data protection mechanisms. The core challenge lies in how to minimize the exposure of data subject identities while maintaining data availability, preventing identity re-identification through data association analysis. At the same time, privacy protection solutions must also meet the strict requirements of power services for data real-time performance and accuracy, ensuring that overprotection does not affect the normal operation of the system and control decisions.

2.4 Compliance and Real-time Performance

Power information systems operate under the dual pressures of compliance and real-time performance. On the one hand, the system needs to meet the compliance requirements of laws and regulations such as the "Cybersecurity Law," the "Data Security Law," and the "Regulations on the Security Protection of Critical Information Infrastructure," establishing a sound security protection system and data protection mechanism. On the other hand, power production control services have extremely high requirements for system real-time performance; the transmission delay of dispatch instructions and the response time of protection devices must be within the millisecond range. This real-time requirement makes many traditional security technologies unusable; for example, deep packet inspection may introduce unacceptable delays, and complex encryption algorithms may affect the timely transmission of control instructions. Therefore, power information security protection must find the optimal balance between compliance and real-time performance, developing lightweight security algorithms and dedicated protection equipment suitable for the characteristics of power services, ensuring that security measures do not affect the normal operation and control performance of the power system.

3. Security Protection Technology System

3.1 Data Secure Transmission and Verification Technology

Secure data transmission in power internet of things communication is the primary aspect of ensuring the safe operation of the system. For multimedia service data such as video surveillance and remote control, the adoption of an end-to-end encryption transmission mechanism based on the

Chinese National Cryptographic Algorithms (SM2/SM4) is crucial. In the video stream transmission process, a lightweight frame-level encryption scheme is employed. This scheme fully encrypts I-frames and selectively encrypts key information such as motion vectors and DCT coefficients of P/B frames, achieving a balance between security assurance and computational overhead control. Simultaneously, a data integrity verification mechanism is constructed based on the SM3 hash algorithm. This generates a Message Authentication Code (MAC) during data transmission, and the receiving end verifies the MAC to ensure that the data has not been tampered with. To further enhance security, a dynamic key update scheme based on Key Derivation Function (KDF) is designed[6]. This scheme periodically updates encryption keys based on session time or data volume thresholds, effectively preventing security risks associated with long-term key usage. After implementation in the smart inspection system of a provincial power company, this scheme successfully resisted replay attacks and data tampering attacks while ensuring real-time video stream transmission (delay increase <50ms).

3.2 Optimization of Intelligent Terminal Access Control

Addressing the characteristics of the power internet of things, such as the large number of terminals, diverse types, and complex access environments, a dynamic access control system based on a zero-trust architecture is constructed. This system adheres to the principle of "never trust, always verify" and establishes a multi-dimensional trust evaluation model centered on identity. First, device fingerprint identification technology is implemented. This involves collecting hardware, software, and behavioral characteristics of terminal devices to generate a unique digital device fingerprint. Second, a continuous identity authentication mechanism is introduced. This dynamically adjusts the trust score during the session by analyzing contextual information such as user operation behavior and device operating status. When abnormal behavior is detected (such as access at unconventional times, attempts to elevate privileges), the system automatically triggers a tiered response mechanism, including requiring re-authentication, restricting access scope, or terminating the session. Implementation in a smart inspection system of a substation showed that this scheme reduced the success rate of unauthorized access attempts by 92% and shortened the average detection time of abnormal access behavior to 3.2 seconds.

3.3 Deep Security Detection and Defense

Covert channel threats in power multimedia communication require defense using deep content detection technology. A multimedia steganalysis model based on deep learning is constructed, employing an architecture combining Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks to extract both spatial features and time series features. This model is trained on a sample library containing samples generated by various steganography tools, enabling effective detection of common steganographic techniques such as Least Significant Bit (LSB) steganography and spread spectrum steganography. Addressing the specific characteristics of power dispatch communication, a multi-modal anomaly detection mechanism is designed to synchronously analyze audio, video, and metadata information, discovering anomalies through cross-modal consistency verification. When suspicious content is detected, the system automatically triggers a tracing mechanism, recording the communication path, traversed network nodes, and processing equipment, providing a complete chain of evidence for security incident investigation. Actual deployment data shows that this solution achieves a detection accuracy of 98.7% for common steganographic techniques, with a false positive rate controlled below 0.5%.

3.4 Intrusion Detection and Collaborative Emergency Response

An intrusion detection and emergency response system based on big data analysis is established. By collecting multi-source data such as network traffic, system logs, and user operations, a normal behavior baseline is constructed for power business scenarios. An unsupervised learning method combining an improved Isolation Forest algorithm and autoencoders is used to achieve effective detection of newly emerging attack types. When a potential threat is detected, the system initiates a collaborative response mechanism: first, the affected terminal is network-isolated to prevent lateral movement; simultaneously, a forensics procedure is initiated to preserve attack-related evidence data; then, a corresponding emergency plan is initiated based on the threat level, including switching to a backup channel and enabling an emergency control mode. To improve response efficiency, a traffic scheduling mechanism based on Software-Defined Networking (SDN) is designed to achieve millisecond-level attack traffic isolation and business traffic rerouting. A pilot project at a local power supply company showed that this system reduced the average time for attack detection from hours to minutes, and reduced emergency response time by 68%, significantly improving the overall security of the system.

4. Key Technologies

4.1 Data Desensitization Technology

Privacy protection in the electric power big data environment needs to go beyond traditional static desensitization methods. Dynamic fusion technology based on k-anonymity and differential privacy provides an effective solution to this problem. This technical system first establishes a data sensitivity grading model, and dynamically adjusts the privacy protection intensity according to factors such as data type, application scenario, and access subject. During implementation, an adaptive k-value selection algorithm is used to optimize the size of the anonymous group in real time based on query frequency and data distribution characteristics, avoiding data utility loss caused by over-generalization. At the same time, a dynamic noise injection scheme based on the Laplace mechanism is introduced to intelligently adjust the noise magnitude according to data sensitivity and query context. In particular, for time-series electricity consumption data, a sliding window mechanism is designed to achieve privacy protection while ensuring data time-series characteristics. Experimental results show that this scheme controls the relative error of data analysis results within 15% under the premise of achieving ε-differential privacy protection, which is significantly better than traditional static desensitization methods. Implementation in a smart electricity consumption analysis project shows that the user re-identification risk is reduced to below 0.3%, while maintaining the availability of data analysis results.

4.2 Privacy-Preserving Application of Federated Learning in Cross-Domain Data Collaboration

In response to the data silo problem that is common in electric power services, federated learning provides a privacy-preserving distributed solution. A federated learning framework based on hierarchical aggregation is constructed to support various business scenarios such as substation equipment monitoring and user electricity consumption behavior analysis. In this framework, local city companies train models locally as clients and only upload model parameters to the provincial center for aggregation. To enhance security, a parameter protection mechanism based on homomorphic encryption is adopted to ensure the confidentiality of model parameters during the aggregation process[7]. At the same time, a differential privacy-enhanced noise addition scheme is

designed to inject an appropriate amount of noise before the model parameters are uploaded to prevent the inference of training data information through model inversion attacks. In response to non-independent and identically distributed (Non-IID) data challenges, an adaptive weighted aggregation algorithm is developed to dynamically adjust the aggregation weights according to data quality and distribution characteristics. In a cross-regional equipment failure prediction project, this framework improved the model prediction accuracy to 92.5% while ensuring that the data of each subject did not leave the domain, an increase of approximately 18 percentage points compared to single-region training.

4.3 Construction of a Security Management System for the Entire Data Lifecycle

The security management of power data needs to cover the entire process from generation to destruction. A full lifecycle security management system based on data lineage tracking should be constructed to achieve transparency and controllability of the data flow process. In the data acquisition stage, embedded security chips and lightweight authentication protocols are used to ensure the authenticity and integrity of the source data. During data transmission, a virtual private channel is constructed based on 5G network slicing technology to achieve isolated transmission of services with different security levels. In the data storage stage, multi-granularity access control policies are implemented, combined with attribute-based encryption (ABE) technology, to achieve fine-grained access authorization based on data attributes and user identity. A trusted execution environment (TEE) is introduced in the data processing links to ensure that sensitive computing processes are carried out in a hardware encryption zone. In the data destruction stage, blockchain technology is used to record destruction operations to achieve auditability of the destruction process. After the implementation of this system in a provincial power company, data violations decreased by 76%, and the average tracking time of data flow processes was shortened from hours to minutes.

5. Conclusion

This study systematically investigates the information security and privacy protection issues faced by power systems in the internet communication environment, and constructs a "proactive defense-privacy enhancement" dual-drive technical system. In terms of security protection, it proposes a data security transmission scheme based on domestic cryptographic algorithms, a dynamic access control mechanism under a zero-trust architecture, a deep detection method for multimedia content, and a collaborative emergency response system based on behavior analysis. In terms of privacy protection, it innovatively combines dynamic anonymization and differential privacy technology, designs a federated learning framework suitable for power scenarios, and establishes a security management system covering the entire data lifecycle. These technical solutions have achieved significant results in the empirical application of a provincial power company, successfully reducing the incidence of security events by more than 75%, and maintaining the efficient operation of business systems while ensuring data privacy.

References

[1] Lin Zhiang, Zhang Yunxuan, Chen Jianbin. Active Risk Warning for Power Network Security Based on Big Data [J]. Electric Power Equipment Management, 2025, (08): 242-244.

[2] Liu Sijun, Huang Xiaokun, Zhou Yue. Research on the Current Situation and Countermeasures of Data Security Protection in Power System [J]. Electrical Equipment and Economy, 2025, (09): 253-255.

[3] Bai Bing, Er Dun, Zhang Jing, et al. Dynamic Bad Information Security Filtering Method for Big Data in Power Information System [J]. Industrial Control Computer, 2025, 38(07): 113-114.

[4] Wang Lin. Research on Power Network Data Security and Privacy Protection Algorithms Based on Hybrid

Encryption [J]. Computing Technology and Automation, 2025, 44(01): 7-11.
[5] Wu Zicheng. Analysis of Power Network Data Security and Privacy Protection Technologies Based on Internet of Things [J]. Application of IC, 2025, 42(06): 328-329.
[6] Chu Yunfei, Wang Yong, Du Xuguang, et al. Digital Grid Middle Platform Data Security Sharing Method for Business Domain [J]. Information Technology, 2025, (05): 162-167+173.
[7] Cui Shunju, Liu Yiqing, Ren Tianyi, et al. Power Internet Business Data Security Transmission Method Based on National Cryptographic Algorithm [J]. Electric Power Equipment Management, 2025, (09): 233-235.