Journal of Electronics and Information Science (2023)
Clausius Scientific Press, Canada

DOI: 10.23977/jeis.2023.080405
ISSN 2371-9524 Vol. 8 Num. 4

Development of Electric Power Information Communication in the Era of Big Data

Zihao Zhao

Information & Telecommunications Company, State Grid Shandong Electric Power Company, Jinan, 250013, China

Keywords: Era of big data; Electric power information communication; Data security; Security threats

Abstract: With the advent of the era of big data, the significance of electric power information communication within power enterprises has grown increasingly important. This paper delves into the development of electric power information communication in the context of the big data era, focusing on the perspective of data security. Initially, we analyze the impact of the big data era on enterprises, along with the opportunities and challenges brought about by big data. Subsequently, we underscore the importance of electric power information communication in terms of data security and discuss the security threats currently faced by electric power information communication. Moreover, we explore the developmental trends in electric power information communication and propose several solutions and recommendations to bolster data security in this domain. Lastly, we summarize the primary content of this paper and provide insights into the future prospects of electric power information communication development.

1. Introduction

With the rapid advancement of information technology and the emergence of big data, enterprises are confronted with the tasks of handling and managing massive volumes of data. Against this backdrop, electric power information communication, as a crucial means of information transmission in power enterprises, plays a pivotal role. Electric power information communication not only facilitates the efficient transmission of large-scale data but also supports long-distance communication, meeting the real-time and security requirements of power enterprises. However, as the volume of big data continues to grow, electric power information communication faces an escalating array of security threats. Consequently, researching the development of data security in electric power information communication becomes particularly significant.

2. The Impact of the Big Data Era on Power Enterprises

2.1. Data-Driven Decision Making

In the era of big data, enterprises are faced with the generation and accumulation of massive amounts of data. This data can encompass information from various channels and sources, such as

customer behaviors, market trends, product sales data, and more. Through the analysis and extraction of insights from this data, enterprises can acquire more comprehensive and accurate information to support decision-making processes. Electric power information communication, as a pivotal means of facilitating large-scale data transmission, enables the consolidation of dispersed internal data within power enterprises. This allows enterprises to promptly collect and analyze data, providing robust support for decision-making.

Within power enterprises, user electricity consumption data can be combined with energy consumption habits and social monitoring data. This combined data can then be transmitted to data centers for analysis, contributing to decision-making in government departments.[1] For instance, this data can aid decisions related to factors such as vacancy rates in residential areas and environmentally non-compliant production. This precise "portrait" of electric power big data offers a comprehensive overview for urban energy efficiency governance. For example, by transmitting data such as overall electricity consumption in a residential area, household energy usage, and the age of buildings to a data center via electric power information communication, and subsequently utilizing big data analysis tools to mine and analyze this data, government authorities can grasp real estate development situations. This facilitates the timely identification of economic risks and effective urban planning.

2.2. Enhanced Quality Services

Fault analysis of power grid equipment is an application scenario that involves transmitting equipment operational data to data centers via electric power information communication for analysis, aiming to improve service quality. For instance, power companies can transmit real-time operational data of power grid equipment to data centers through electric power information communication. Subsequently, this data can be subjected to analysis and exploration using big data tools. By analyzing this data, power companies can identify patterns and trends in equipment malfunctions, predict potential faults in advance, and take corrective measures to enhance the reliability and stability of power grid equipment. This, in turn, facilitates the provision of high-quality power services. For example, when data analysis reveals frequent equipment failures in a particular area, a power company can dispatch maintenance personnel to reinforce inspections and maintenance in that region.[2] This reduces the frequency of failures and downtime, ultimately enhancing users' electricity consumption experience and satisfaction. Such analysis and prediction aid power companies in optimizing maintenance plans, improving equipment reliability, and offering customers more dependable and stable power supply services.

2.3. Supply Chain Optimization

In the era of big data, enterprises can optimize supply chain management through data exchange and sharing across various stages of the supply chain using electric power information communication. Power enterprises can integrate and analyze data from different stages, including power generation plants, transmission lines, substations, user distribution, and more, using electric power information communication. This integration facilitates precise supply-demand matching and efficient resource utilization, resulting in cost reduction and increased efficiency. For instance, power enterprises can transmit electricity consumption curve data for peak, off-peak, and average periods to data centers through electric power information communication. Subsequently, big data analysis tools can be utilized to mine and analyze this data. Through analysis, adjustments can be made to purchased electricity quantities to achieve supply-demand balance, thereby optimizing the supply chain.[3]

3. The Importance of Electric Power Information Communication in Data Security

3.1. Ensuring Secure Data Transmission

Power plants, as crucial energy suppliers, need to transmit data to power enterprises to ensure the normal operation of power supply. In this process, ensuring the security of data transmission becomes paramount. This is because such data may contain sensitive information about the internal operational status of power plants, equipment maintenance details, and more. To guarantee the security of data transmission, electric power information communication can implement a series of security measures. Firstly, encryption techniques can be employed to encrypt data, ensuring that even if intercepted during transmission, the data remains unreadable. Secondly, identity authentication can be utilized, ensuring that only authorized users or entities can access and transmit data. Additionally, access control measures can be implemented to restrict different users or entities' access permissions, preventing unauthorized personnel from tampering with or leaking data. For instance, power enterprises can transmit real-time operational data and equipment status information of power plants through electric power information communication. Such data is of vital importance to power enterprises, aiding them in monitoring power plant operations promptly and making necessary adjustments. During transmission, data encryption can be employed to ensure data confidentiality. Simultaneously, identity authentication via electric power information communication ensures that only authorized personnel can access and receive the data. These security measures guarantee the integrity and security of power plant operational data against unauthorized tampering, interception, or leakage.[4]

3.2. Security in Data Storage and Processing

In the era of big data, power enterprises face the need to store and process massive amounts of data, including valuable business information and user privacy. Therefore, a range of security measures, encompassing physical, network, and system security, needs to be adopted in electric power information communication. Suppose power plants store internal operational data, equipment statuses, and customer information in a data center, utilizing this data for operational management and customer services.[5] In order to safeguard the security of this data, power enterprises can enhance the security measures of data centers. Firstly, physical security can be elevated by increasing monitoring equipment and implementing security alert systems, ensuring that only authorized personnel can access the data center and perform operations. Secondly, network security can be bolstered, including the establishment of firewalls and intrusion detection systems to prevent unauthorized individuals from intruding into the data center via the network. Additionally, power enterprises should strengthen system security, such as limiting administrator privileges, regularly updating software patches, and implementing data backup and disaster recovery measures to address potential system failures or data losses. Through these security measures, power enterprises can ensure the security of power information and customer data stored in data centers. For instance, access control technology can be employed, ensuring that only authorized personnel can access and process the data. Encryption techniques can be utilized to protect the confidentiality of personally identifiable information. Moreover, regular data backup and disaster recovery can reduce the risk of data loss, ensuring data availability and integrity.[6]

3.3. Legal Compliance in Privacy Protection

With increasing occurrences of data breaches and violations of personal privacy, protecting user privacy has become both a legal and societal responsibility for enterprises and organizations. In the era of big data, electric power information communication, as a crucial means of data transmission for power enterprises, must adhere to relevant laws, regulations, and privacy protection standards

when collecting and transmitting user personal information, social relationships, and other data. For instance, power enterprises collect and transmit personal information and electricity consumption data of users through electric power information communication. To protect user privacy, power enterprises must explicitly inform users of the specific purposes of data collection and obtain their express consent during the data collection process. Simultaneously, power enterprises must implement reasonable data security measures to ensure the confidentiality and integrity of user data during transmission. To meet legal requirements for data privacy, power enterprises can establish privacy policies, clearly informing users about the collection and usage of their personal information, as well as how data will be protected and processed. During data transmission, encryption techniques and security protocols can be employed to prevent unauthorized access or tampering of user data. Additionally, in terms of data storage, power plants should establish secure databases and access control mechanisms, limiting access and processing of user data to authorized personnel.

4. Security Threats Faced by Electric Power Information Communication

4.1. Network Attacks and Hacker Intrusions

Network attacks and hacker intrusions are among the primary security threats faced by electric power information communication. Hackers may employ various methods to attack the power system's network, such as launching Distributed Denial of Service (DDoS) attacks to cause system paralysis, using SQL injection techniques to retrieve sensitive information from databases, or conducting Cross-Site Scripting (XSS) attacks to steal user login credentials. For instance, hackers could employ DDoS attacks to target an electric power enterprise's information communication system, leading to massive disruptions in the operation and management of power equipment, consequently impacting the stability and reliability of power supply services.

4.2. Identity Authentication and Access Control Issues

Insufficient identity authentication and access control within electric power information communication can also pose security threats. Failure to properly verify user identities or restrict unauthorized access could lead to issues such as data leakage, data manipulation, and unauthorized operations. For example, an unauthorized employee using someone else's account logs into the electric power information communication system, gaining control privileges over power equipment. This employee might then engage in unauthorized actions, such as shutting down power supply to a specific area, resulting in power interruptions and failures.

4.3. Data Tampering and Data Loss

During data transmission in electric power information communication, there is a risk of data tampering and loss. Hackers can use methods like Man-in-the-Middle attacks to alter data content, or data might be lost during transmission, resulting in incomplete or inaccurate data. For instance, a hacker executes a Man-in-the-Middle attack, intercepting purchase data between a power enterprise and a power plant. The hacker manipulates price information in the order data, causing the power plant to miscalculate pricing as per incorrect specifications, leading to financial losses for the enterprise.

4.4. Physical Security Threats

In addition to cyber threats, electric power information communication also faces physical security threats. Unauthorized individuals gaining access to power facilities could sabotage equipment, steal critical components, or manipulate device configuration, thereby affecting the security and operational stability of electric power information communication. For example, a hacker disguises

themselves as a power equipment maintenance personnel and quietly disassembles and damages a critical network device. This results in the failure of the electric power information communication system, impacting the power enterprise's supply services.

4.5. Software Vulnerabilities and Untimely Patching

The software used in electric power information communication systems may have vulnerabilities that hackers can exploit if not promptly patched. Therefore, timely software updates and patching are critical for ensuring security. For instance, open-source software utilized may have publicly disclosed vulnerabilities. However, if system administrators fail to update patches in a timely manner, hackers can exploit these vulnerabilities to successfully breach the system and access sensitive user data.

5. Electric Power Information Communication Trends and Solutions

5.1. Application of Data Encryption Techniques

5.1.1. Symmetric Encryption Algorithms

Symmetric encryption algorithms use the same key for both encryption and decryption operations. AES (Advanced Encryption Standard) is one of the widely adopted symmetric encryption algorithms. It operates based on block cipher principles, dividing data into fixed-size blocks and applying transformation functions repeatedly for encryption and decryption. For example, AES algorithm can be used to encrypt a data signal requiring confidentiality, ensuring that only authorized users possessing the key can decrypt and access its content.

5.1.2. Asymmetric Encryption Algorithms

Asymmetric encryption algorithms use a pair of distinct keys for encryption and decryption operations. The public key is used to encrypt data, while the private key is used to decrypt it. Applications of asymmetric encryption include key distribution, digital signatures, and identity authentication. Common asymmetric encryption algorithms include RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography). For instance, in an electric power information communication system, asymmetric encryption algorithms can be used for secure key exchange, ensuring that keys are not compromised during transmission.

5.1.3. Digital Signature Technology

Digital signature technology involves using a private key to sign data, and the recipient can verify the authenticity and integrity of the signature using the corresponding public key. This prevents data tampering during transmission. For example, in an electric power information communication system, digital signature technology can be employed to sign important data packets, ensuring data integrity and trustworthiness. For instance, an electric utility company sends power usage data to a power dispatch center. To secure this data, the utility company can encrypt the power usage information using the AES algorithm. Only the power dispatch center with the corresponding key can decrypt the data for processing, ensuring that even if intercepted, the data remains unreadable to hackers.

5.2. Establishment of Robust Identity Authentication and Access Control Mechanisms

5.2.1. Multi-Factor Authentication

Multi-factor authentication involves using various authentication methods to enhance system security. By employing multiple factors such as passwords, biometric features (e.g., fingerprints or facial recognition), and hardware tokens (e.g., smart cards), the likelihood of attackers obtaining

legitimate user identities is reduced. For example, operator authentication to access critical equipment can require a correct password and biometric verification via fingerprint recognition, ensuring only authorized personnel can access the critical devices.

5.2.2. Role-Based Access Control (RBAC)

RBAC is an access control mechanism based on roles and responsibilities, assigning appropriate access privileges based on user roles and responsibilities. By allocating users to different roles and defining corresponding permissions for each role, fine-grained access control can be achieved. For instance, users can be categorized into roles such as administrators, operators, and maintenance personnel. Administrators have the highest privileges, accessing and managing all system resources; operators can only access the necessary critical equipment and related data; maintenance personnel can troubleshoot and maintain devices. Through the RBAC mechanism, user access to specific resources is restricted, enhancing system security.

5.2.3. Logging and Auditing

Implementing comprehensive logging and auditing mechanisms helps monitor and track all user operations and access behaviors. This aids in identifying potential security incidents and conducting investigations. User login times, IP addresses, executed actions, and accessed data should be logged. Regular audits examine logs for anomalies or non-compliant activities. For example, if a user repeatedly attempts to access resources beyond their authorization level, alerts are triggered, and appropriate measures are taken to protect the system.

5.3. Data Backup and Recovery Mechanisms

5.3.1. Regular Data Backup

Critical data in the electric power information communication system should be regularly backed up to a secure location, such as offline storage media or remote data centers. This allows recovery to the latest backup in case of data corruption, loss, or attacks. Critical data should be backed up daily to two data centers located in different geographic locations. If one data center experiences a failure or attack, the other can still provide backup data, ensuring business continuity.

5.3.2. Redundant Storage and Disaster Recovery Technology

Redundant storage and disaster recovery technologies provide backups of data on multiple devices or locations to ensure data availability and integrity. For example, using RAID technology can provide hard drive fault tolerance. Furthermore, deploying data centers in multiple geographic locations achieves disaster recovery. Key data should be stored on multiple servers with data redundancy achieved through RAID technology. If one hard drive fails, other drives maintain data integrity, ensuring system operations continue.

5.3.3. Disaster Recovery Plan

Establishing a robust disaster recovery plan helps the electric power information communication system quickly recover normal operations in the face of disasters or attacks. This plan should include emergency response steps, data recovery processes, and testing procedures. A comprehensive disaster recovery plan defines responsibilities, emergency response steps, and communication processes for various disaster scenarios. Regular disaster drills test the recovery process to ensure quick and effective business recovery in the event of a disaster.

5.4. Enhancing Continuous Monitoring and Identification Capability

5.4.1. Real-time Monitoring and Log Analysis

Real-time monitoring of network traffic, system logs, and behavior analysis can promptly detect abnormal activities and security incidents. For instance, Intrusion Detection Systems (IDS) can be employed to monitor network traffic in real time, detecting and alerting for anomalous behavior. Simultaneously, analyzing system logs can uncover potential security threats and signs of attacks, enabling quick measures to prevent further escalation.

5.4.2. Threat Intelligence and Vulnerability Management

Obtaining up-to-date threat intelligence and vulnerability information and conducting vulnerability scans and assessments can help identify potential security risks and apply timely remedies. This includes establishing collaborations with relevant security vendors and organizations to regularly obtain the latest threat intelligence and vulnerability information. Additionally, periodic system scans using vulnerability assessment tools can identify existing vulnerabilities in the system and apply timely patches to reduce potential attack risks.

5.4.3. Security Incident Response and Emergency Planning

Establishing a sound security incident response and emergency plan helps the electric power information communication system respond and recover swiftly in the face of security incidents or attacks. This involves crafting detailed security incident response and emergency plans, including defining responsible individuals, emergency response steps, and communication processes. Conducting emergency drills ensures that the team can collaborate efficiently and act promptly in the face of security incidents.

6. Conclusion

This paper has explored the development of power information communication in the context of the big data era from the perspective of data security. Through the analysis of the impact of the big data era on enterprises, the importance of power information communication, security threats, and solutions, we have recognized the significance of power information communication in ensuring data security. In the future, we should continuously strengthen research and innovation in power information communication, enhance data security capabilities, and provide reliable support for the development of power enterprises in the era of big data.

References

[1] Tang, Z., & Jie, D. (2021). Development Prospects of 5G Mobile Communication Technology in the Era of Big Data. Yangtze Information Communication, 34(11), 212-214.
[2] Qin, Z., & Jing, H. (2018). Research on Power Information Communication Early Warning Technology Based on Big Data. Computer Products and Distribution, (07), 78.
[3] Zhang, Y. (2017). Evaluation of Power Communication Networks in the Era of Big Data. [Master's thesis, Nanjing University of Information Science & Technology].
[4] Peng, X. (2022). Analysis of Power Communication Network State Awareness Based on Big Data. Electrical Application, 41(10), 25-30.
[5] Zhu Mingyue (2015). Thinking and Exploration of Power Information Technology in the Era of Big Data. Information and Computers: Theoretical Edition, (5), 2.
[6] Yang, N. (2022). Case Sharing of Power Communication Optical Cable Big Data Analysis Platform. China New Communications, 24(24), 13-15.