Journal of Network Computing and Applications (2025)
Clausius Scientific Press, Canada

DOI: 10.23977/jnca.2025.100103
ISSN 2371-9214 Vol. 10 Num. 1

Computer System Security and Power Data Network Integrated Security Strategy Analysis and Optimization

Fengyi Zhao

Business Operation, Intercontinental Exchange, Atlanta, 30328, Georgia, United States
fengyi9803@gmail.com

Keywords: Computer system; Power data network; Security policy analysis

Abstract: In the context of the rapid development of information technology, computer network technology in the power industry, although it provides important support for daily operations, is also facing serious network security threats such as malware, hacker attacks and system vulnerabilities. This paper aims to comprehensively analyze and optimize the security strategy of power information system to ensure its security and efficiency in the big data environment. By clarifying the functional requirements and network security architecture of power information systems, we identify specific security standards and propose innovative technical solutions including multi-level security protection, high-strength encryption technology, artificial intelligence monitoring and physical security measures. Build a comprehensive network security operation and maintenance management platform, and conduct regular hardware and software maintenance and security assessment to cope with evolving network threats. By combining big data technology with the security management of power information system, this paper hopes to provide an effective scheme for relevant decision-making bodies, improve the security protection capability of power information system, ensure the integrity and effectiveness of data, and lay a foundation for the sustainable development of the power industry.

1. Introduction

Modern electronic information systems are facing more and more problems in data security, especially network threats. Ensuring the protection of confidential information does not only mean preserving its integrity and confidentiality; This includes important user activities, such as retention of records, access to information and financial transactions, and the fact that access, disclosure and discovery of data must take place without prior authorization. This requires a strong security structure that directly affects the reliability of the system and creates trust between users. In order to reduce the risk of data loss, such a security infrastructure must focus not only on the flexibility of the system, but also on the trust of the users, which means that the system operates properly and reliably.

Extortion, online Trojan horses and worms infiltrate the digital space and seriously threaten the security of electronic information systems. These types of malware often amplify system vulnerabilities via unreliable websites or applications. This threat exacerbates the entire system and can even lead to its collapse. To effectively manage these risks, it is essential to have a

comprehensive security infrastructure that allows us to monitor deficiencies, draw attention to them, and integrate the latest developments into security functions. The use of real-time testing is essential to quickly identify and respond to potential threats on the Internet. This proactive approach ensures the maintenance and continuity of systems, as well as their integrity and proper operation.

This study highlights the importance of building strong security structures for electronic information systems, especially in big data environments. Thorough risk assessment and sophisticated empathetic protection mechanisms significantly reduce vulnerability to cyber threats. Ensuring the integrity and efficiency of energy information systems is essential to laying the foundations for the long-term growth and sustainable development of the sector. Increased collateral helps stabilize the system to ensure a sustainable recovery, a successful future and sustainable development of the sector.

2. Related Research

Given that the industrial landscape can still be characterised by technological advances, the growing dependence of the energy sector on information systems raises new security issues, particularly in light of the rise of online fraud. In recent years, the possibilities for computer fraud have become more varied and more complex. Cyber criminals often use digital platforms as client agents or law enforcement agencies, breaking trust and compromising financial security. Not only is the growing threat undermining public confidence, it is also a serious obstacle to the security of the energy sector and a serious risk to its stability and growth.

With rapidly changing technologies, optimizing energy systems is essential, especially to meet the demands of the big data era. As modern systems strive to process large amounts of energy related data, there is increasing evidence of improving data management methods. To be effective, companies in the energy sector should focus on protective measures, focusing on the identification and prevention of cyberfraud, which represents a significant threat to data integrity and financial stability. This proactive approach is essential to ensure the proper functioning and security of energy information systems in an increasingly interconnected digital world. This step is necessary to protect the organization and its users.

Law enforcement works with stakeholders to strengthen law enforcement, improve public information and raise awareness about the protection of personal information and assets. Optimizing information systems for power generation requires technologies that improve security. By integrating advanced information technology, energy companies can proactively address complex threats while meeting business needs. This comprehensive security strategy will provide a solid guarantee for the sustainable development of the power industry and ensure that the rights and interests of users are effectively safeguarded while the rapid development is taking place. To solve the problem of incomplete online measurement of power grid voltage, YChai team proposed a local coordinated voltage optimal control strategy that combines local optimization and real-time coordinated control[1]. The X Yang team carefully constructed an intelligent scheduling engine and a condition monitoring and early warning system, which significantly improved the real-time response, decision optimization and active security defense capabilities[2]. S Yuan's team proposes a systematic risk-based approach that combines traditional security risks with emerging C2P attack risks[3]. The YMa team proposed a method for safe sharing of monitoring data of hydropower station operation and maintenance[4].

3. Optimize and Implement Security Management Strategies for Computer Network Systems in the Power Industry

3.1 Firewall

In order to effectively deal with the risks of computer network systems, it is essential to optimize the network security management strategy, which will lay a solid foundation for creating a safe, civilized and green network environment. The implementation of intelligent firewall is the key to prevent external threats. By dividing the network into internal and external networks, firewalls can set up secure accounts for internal networks and strictly limit unauthorized access.All external access must be strictly controlled to ensure that only authorized users have access to protected data, to prevent unauthorized access and to strengthen data protection.

Focusing on strengthening the firewall. By combining advanced robotics with behavioral analytics, the company can track traffic in real time and identify potential viruses and anomalies. Improve response speed and improve the effectiveness of safety measures. Timely prevention of external threats is essential to mitigate security risks. Regular assessment and updates of firewalls, along with security protocols, are vital to counteract emerging threats and evolving attack strategies. This ongoing process of evaluation and improvement is crucial for safeguarding the integrity of the entire system, ensuring it remains resilient against new vulnerabilities and maintaining overall security.

The computerization of higher technische hochtechnische is one of the most important aspects of computerization and the konzentration of all the stehenden werkzeuge and mitarbeiter. This is the first time that have had a debate on energy policy in the European Community. This is an integral part of the schutz, which is positive in terms of social security and social security. The branch can be divided into three parts.

3.2 Improving Network Technology

Enhanced data encryption plays an important role in improving it security. The main protection mechanisms against unauthorized access and threats in cyberspace. Most of the data is transmitted in binary and the system relies on ASCII coding to convert characters into robots readable signals. The process underlines the urgent need to protect sensitive information in an environment to ensure that encryption is effective enough to prevent data transmission. Maintaining the integrity and confidentiality of information is an essential part of cybersecurity.

The modern nature of kryptography is a reflection of the world, the world with sensiblen information, the world with knowledge, the world with knowledge, the world without knowledge and the world without knowledge. The modern kryptography arbeitet in dem prinzip, lesbare daten en eine verschlusselte umzuwandeln, Die ohne den richtigen dechiffrierschlusel so gut wie unm o glich ist. That is why it is important for the integrity of the data to be sensitive, and that is why it is important for the integrity to be sensitive. This is the beginning of a new era.Security measures are essential to reduce risks in digital systems and maintain trust in digital systems.

The algorithm must be updated regularly to deal with new threats. Cybercriminals have developed more sophisticated ways to circumvent security measures, and companies must proactively identify and fix vulnerabilities. A proactive strategy for regular assessment and timely update takes a crypto organisationsschutz approach to enhancing change against risk to protect sensitive data and the long-term flexibility of a system, which is to adapt to changing cybersecurity challenges.

The effectiveness of encryption depends on the algorithm chosen and its integration into the broader security framework, and the port has achieved greater security and continuous control, and

the system "wants to be secure." By implementing these additional measures, the IMF has created a more flexible and robust protective threat that provides greater flexibility and security.

An important aspect of improving security is the importance of providing employees with information about encryption and data protection. Workers must be aware of the risks of weak security protocols and view encryption as an important safeguard against such threats. Fostering a culture of security can greatly reduce the sharing of data due to human error. This proactive approach provides employees with the necessary expertise, improves the overall security structure, and creates a flexible organization.

Is more encryption just a technical requirement? This is an important strategy to prevent unauthorized access and data loss. The Security Council for Complex Cryptography Technologies provides a comprehensive approach to better manage it security in a rapidly evolving digital environment and enhance user confidence in protecting their information.

Modern cybersecurity experts use complex mathematical structures to make it more difficult for attackers and improve security.Modern cryptographic models include space-time object model and evolutionary model. While the "e" 22 is very important in terms of memory efficiency, allowing many objects to share Pointers and save space, their complex combinations can make data output and content difficult.In contrast, the spatial entity model, through the repeated use of common nodes, can modify one object without affecting other objects, significantly enhancing the data maintainability.

When constructing the computer network security management model, the advantages of these two models can be integrated to design an effective solution that not only saves storage space but also facilitates maintenance. This comprehensive method can not only meet the operation requirements of computer network security, but also improve the confidentiality level of internal data in the system. The combination of cutting-edge encryption technology and multi-level protection mechanism will be the key to ensure the safe and stable operation of network system. These policies provide greater protection for your critical information, improve the security of your network, and ensure the efficiency of your system.

4. Optimization of Power Information System Network Security Technology

4.1 Optimization of Mass Data Storage Technology and Security Analysis of Power Information System

When designing data storage strategies for energy systems, it is important to understand how big data will impact the energy sector in the long term. Understanding this concept is critical to developing high-performance and efficient data storage solutions. The implementation of this framework significantly improves the speed of data transfer across disks and optimizes the memory utilization within the system core. It speeds up the speed of data movement, improves the overall efficiency of the system, and ensures that the storage operation can meet the needs of modern data environment.

Fostering collaboration between different stakeholders, such as IT specialists, data analysts, and energy industry experts, is critical to ensuring that storage solutions are not only technically feasible, but also aligned with the organization's strategic goals. By emphasizing the flexibility and flexibility of storage structures, organizations can better define themselves to adapt to future developments and the changing industry landscape.

The effectiveness of such speicherlosungen depends on a comprehensive approach to issues and may be required for vorhersagende. To carefully plan and implement the system can not only improve the efficiency and data storage efficiency not only secure and reliable electronic information system overall. Taking this proactive approach will lay a solid foundation for the

further development of the big Data energy sector and ensure that the infrastructure meets new demands.

When designing the power supply system, the standard buffer must be added to meet the requirements of equipment data reading. In view of this, it is considered necessary to minimize the risk of data loss and buffer errors caused by buffer size errors. The design must be improved to comply with the security rules applicable to certain energy information systems. By increasing data efficiency, you can maximize the use of data by emphasizing the need for Internet security. Such planning and comprehensive implementation will provide a solid foundation for an expansive and integrated security strategy for electronic information systems.

The design process must not only meet existing operational requirements, but also take into account future developments and evolving safety challenges to ensure the sustainability and effectiveness of the system over time. The precise integration of these elements will ultimately improve the performance of the entire infrastructure.

In order to solve the possible problems of large format storage, the relevant service departments should develop system improvement strategies. These strategies should include not only technological advances, but also a fundamental adjustment to the effectiveness of managementprozessen approach and the basis for formulating policies that are essential to ensure EIS capability in developing big data security systems and effective management of large data. This will strongly support the sustainable development of the energy sector and the transition to rational development.

4.2 Research on Mass Data Retrieval Technology and Security of Optimized Power Information System

The wider distribution of users and their different needs present a significant challenge for power companies to manage the large amounts of data embedded in electrical information systems. Given the growing need for real-time monitoring and response, the adoption of advanced data collection has become an important aspect of the overall optimization of information systems. Optimizing data access not only speeds up access, but also improves the security of the entire system.

Using advanced data collection technology, managers and users can quickly obtain the information they need to conduct comprehensive studies of energy consumption and power demand trends in different regions. Access to real-time data not only improves management efficiency, but also improves special monitoring of power consumption, ensuring the safety and stability of the entire system.

In the extraction process, it is vital for personnel to grasp the representation and application of the data to utilize the information efficiently. Effective mechanisms for retrieving substantial volumes of data from electronic systems must be intricately connected to advanced big data storage technologies to combat the growing complexity of cybersecurity threats. By implementing this holistic approach to optimization, the energy sector can enhance its capacity to tackle security challenges while fostering sound governance practices that support sustainable growth over the long term.

5. Conclusion

This process not only involves the effective storage and management of massive data to prevent information leakage, but also actively demonstrates the security advantages of power information systems. Cybersecurity technologies based on big data are important in improving the security of data storage, processing and comprehensive analysis, which is particularly critical to meet the sustainable development goals of relevant sectors.

It is very important to further optimize the security management strategy of the network system and establish a safe, civilized and green network environment. It is necessary to deploy efficient firewalls and improve information encryption technology, build a comprehensive information transmission protection mechanism, enhance data security through multi-level encryption means, resist various potential malicious attacks, and constantly strengthen the data confidentiality of computer network systems. Use the intelligent monitoring and analysis capabilities of artificial intelligence technology to optimize the network security management system to improve the efficiency and accuracy of response to security incidents. It is necessary to strengthen the supervision of the network environment, improve laws and regulations, strictly crack down on cyber crimes, and enhance the public's awareness of cyber security through education and publicity. Regular hardware maintenance to ensure the implementation of physical security protection measures, the construction of a comprehensive security system, in order to effectively achieve the long-term safety and stable operation of the power information system.

References

[1] Chai Y, Liang T, Dong Y, et al. Local-coordinated voltage optimal control strategy of integrated PV and ESS system in distribution networks with π-type network simplification[J]. Electric Power Systems Research, 2024, 231. DOI:10.1016/j.epsr.2024.110350.

[2] Yang X, Jia K, Peng Z. Construction of integrated network order system of main distribution network based on power grid operation control platform[J]. Energy Informatics, 2024, 7(1): 1-27. DOI:10.1186/s42162-024-00368-6.

[3] Yuan S, Reniers G, Yang M, et al. Integrated management of safety and security barriers in chemical plants to cope with emerging cyber-physical attack risks under uncertainties [J]. IEEE, 2024.

[4] Ma Y, Hong L, Qin T, et al. Research on Monitoring Data Security Sharing Method for Hydropower Station Operation and Maintenance [J]. IOP Publishing Ltd, 2022. DOI:10.1088/1742-6596/2294/1/012009.