Research on Power Network Security Assurance Based on Artificial Intelligence and Data Mining

Zhu,Tao

Nanjing University of Posts and Telecommunications, Nanjing, Jiangsu, 210000, China

Abstract: The development of electric power network security system has been a very important research field in China, because the development of electric power network security is not only related to the daily life of nationals, but also affects the sustainable development of the whole society of China. In the information society, science and technology continue to develop, and artificial intelligence technology and information mining technology are widely used in electric power network safety and security. Based on this, this paper firstly introduces the basic concepts of artificial intelligence and data mining technology, and then discusses the current status of the application of artificial intelligence and data mining in electric power network safety and security. It analyses the practical application of key areas such as risk assessment, intrusion detection, and threat intelligence, and provides an in-depth analysis of the challenges in dealing with ever-changing attack methods, data privacy protection, decision-making transparency, system compatibility, and real-time response. Finally, this paper proposes targeted strategies to improve the overall security and intelligence of the power network through algorithm optimisation, privacy protection, decision transparency, system upgrades and resource allocation optimisation. Building a more adaptable and secure power network security system can effectively respond to complex and ever-changing cyber threats, promote the intelligent and modern development of the power system, and is of great practical significance.

Keywords: Artificial intelligence; Data mining; Power network security

DOI: 10.62639/sspjinss04.20240104

The so-called Artificial Intelligence, also known as AI, is a new technological science that specializes in the study and development of theories, methods, techniques and application systems for simulating, extending and expanding human intelligence. The so-called data mining is to extract useful information from a large amount of data, so as to discover patterns and rules hidden in the data to provide support for decision-making. Nowadays, with the development of information society, these emerging technologies are gradually introduced into various industries. Among them, the application of artificial intelligence and information mining technology in power network security has attracted much attention. Power network security incidents mainly include network security behaviors caused by viruses as well as network attacks and network intrusions, which can cause certain harm to power networks and information systems. In addition to bringing certain convenience to power network security, the addition of emerging technologies also brings many security risks.

1. Overview of Artificial Intelligence and Data Mining Technologies

(1) Artificial intelligence technology

Artificial intelligence (AI) is a technology that enables machines to simulate, expand and even partially replace human intelligence. It allows machines to autonomously analyse, make decisions and learn in complex

(Manuscript NO.: JINSS-24-4-1002)

About the Author

Zhu,Tao (1982-05), Male, Han ethnicity, from Lianyungang City, Jiangsu Province, received the B.Eng. degrees in computer science and technology from the Nanjing University, Nanjing, China, in 2006, received the M.Eng. degrees in Computer Technology from the Wuhan University, Wuhan, China, in 2018, and he is currently pursuing a Ph.D. degree with the School of Computer Science at Nanjing University of Posts and Telecommunications, Nanjing, China.

environments. AI covers subfields such as machine learning, deep learning, natural language processing and computer vision. Computers can rely on these technologies to execute routine instructions and recognise, reason and generate intelligent behaviour. Machine learning is the core technology in the implementation of AI. It enables computers to autonomously 'learn' from data and continuously optimise models by analysing data and extracting patterns. Deep learning is an extension of machine learning based on a multi-layer neural network structure, which enables computers to achieve high accuracy in image recognition, speech recognition and other fields, and even surpass human performance in visual and language comprehension tasks.

The goal of AI technology also includes giving machines the ability to process unstructured data, so that they can excel at tasks such as natural language processing and intelligent reasoning. For example, computers can understand and generate human language with the aid of natural language processing technology, while computer vision gives machines the ability to 'see the ability to 'see', which is widely used in scenarios such as autonomous driving and security monitoring. The rapid development of AI technology is inseparable from the support of big data and powerful computing resources. Large-scale data-driven model training, coupled with cloud computing and distributed computing, enables AI to process massive amounts of data in a short period of time, achieving efficient prediction and decision-making. Today, AI has been widely used in fields such as healthcare, finance, and industrial manufacturing, bringing profound impact and technological innovation to various industries.

(2) Data mining technology

Data mining is a technology that analyses large amounts of data to discover valuable patterns, trends and relationships, with the aim of turning the information hidden in the data into decision support. With the development of informatisation and digitalisation, the amount of data has grown explosively, and data mining technology has become a key means of effectively utilising data assets. This technology combines statistics, machine learning and database technology to help people extract knowledge with practical application value from vast amounts of data. The core methods of data mining include classification, clustering, association rules and regression analysis. Classification technology uses labelled data to train a model to help predict the category of unknown data. It is often used in credit assessment and risk prediction. Clustering groups data and identifies natural patterns of aggregation in the data, so it is widely used in customer segmentation and image processing. Association rules can help reveal the association between data items, and are extremely effective in market basket analysis (e.g. 'customers who buy beer also often buy potato chips'). Regression analysis is used to predict trends in continuous variables such as house prices or sales.

In practice, data mining involves the steps of data collection, pre-processing, mining modelling and result analysis. First, the data needs to be cleaned and transformed to ensure accuracy and consistency. Algorithms then process the pre-processed data to uncover potential patterns. Decision-makers can use this knowledge to optimise decision-making processes and formulate strategies based on the results of the analysis. Today, data mining is widely used in industries such as commerce, healthcare, finance, and electricity. For example, in the electricity system, data mining is often used to identify power usage patterns and optimise power dispatching. Financial institutions use data mining to analyse customer behaviour and carry out targeted marketing. In short, data mining not only extracts information from data, but is also an important means of achieving data-driven decision-making and improving industry intelligence, driving the digital and intelligent development of various fields.

2. Current Status of the Application of Artificial Intelligence and Data Mining in Power Network Security

(1) Risk assessment and prevention

The risks of the power network system include the internal security risks of the power system, the risks of the network equipment and the risks in the network operation and management process. Due to the addition of artificial intelligence and data mining technology, it can efficiently and accurately assess the network risks in the power system, and also prevent potential threats and risks in the system, so as to guarantee the security of the network system. Because artificial intelligence and data mining technology can collect and organize a large amount of historical data, and at the same time, analyze and interpret these data to dig out the hidden inner laws, and then analyze and predict the possible network security problems in the future according to these laws. So it can effectively help the power network system for risk assessment and prevention.

(2) Intrusion detection and response

The application of artificial intelligence and data mining technology has greatly improved the real-time performance and responsiveness of the system. Traditional security protection methods often rely on predefined rules and features, making it difficult to respond to new and hidden cyberattacks. However, with the help of AI and data mining technology, the system can perform in-depth analysis of historical data and the current environment, identify abnormal patterns in large amounts of data, and quickly locate potential threats. AI models can identify signs of intrusion in advance based on irregular traffic or behaviour patterns, providing early warnings to administrators and enabling the system to respond faster[3]. In terms of response measures, AI can quickly generate response strategies and implement corresponding isolation, blocking and other defensive measures. Since the power network system is related to public safety, any intrusion may cause serious consequences, so the timely response of AI technology is very important in this scenario. The intelligence of intrusion detection and response not only reduces delays and errors in manual operations, but also enables the power system to more effectively prevent complex threats.

(3) Threat intelligence analysis

The threats facing power networks are diverse, and new attack methods are emerging all the time. It is difficult to summarise and store all threat information using manual memory and experience. AI technology can establish a memory bank based on the analysis of historical threat data, and gradually enhance the identification and classification capabilities in threat intelligence analysis. The memory function of AI is not only reflected in the analysis of historical data of a single event, but also relies on pattern recognition and linkage analysis to connect multiple events and discover potential correlations. When a new attack is detected, the AI system can quickly compare it with previous threat data to infer similar attack paths or potential motives, providing decision-makers with early warnings and reference for response[4]. Therefore, AI-driven threat intelligence analysis has established a more robust security barrier for the power system. The system can quickly track emerging threats and enhance the security immunity of the power network.

(4) Intelligent monitoring and optimisation

In terms of intelligent monitoring and optimisation, artificial intelligence and data mining provide power networks with 24/7, real-time monitoring capabilities. This zero-gap monitoring mode is almost impossible to achieve in traditional power systems. AI technology can analyse the parameters and behaviour patterns of network systems in real time, automatically detect abnormal changes, quickly determine the possible causes, and take optimisation measures in a timely manner. Unlike the traditional approach of relying on manual monitoring, AI systems can actively adjust resource allocation, adjust system configurations, and immediately correct system parameters when abnormal data fluctuations are detected. When it detects a sudden increase in system load or abnormal traffic, AI can optimise traffic distribution or activate a backup plan in time to prevent system crashes or overloads. In addition, the AI system can learn patterns in daily monitoring data and continuously optimise monitoring processes based on this, making the safe maintenance of power networks more efficient.

(5) Enhancing the autonomy and adaptability of the network

Artificial intelligence can be based on the analysis of historical human operating procedures to learn and imitate human behavior and decision-making processes, and can make decisions autonomously according to the real situation. In the face of a variety of network complete risks and threats, the technology can help the network system to solve and adapt autonomously, so as to improve the defense ability. This is due to the introduction of artificial intelligence technology and data mining technology can improve the autonomy and self-adaptation of power networks.

3. Artificial Intelligence and Data Mining in Electric Power Network Security Application Challenges

(1) It is difficult to deal with complex and ever-changing attack methods

The continuous upgrading of cyberattack methods has made the security of power networks face unprecedented challenges, and it can be said to be unpreventable. Existing artificial intelligence and data mining technologies can perform reasonably well in defending against traditional threats, but they seem to be inadequate when dealing with new and mutated attacks. In addition, today's attack methods are becoming more and more complex and covert, and some even have the characteristic of a chameleon that can disguise itself as normal operation. Although AI technology is good at discovering patterns from historical data, it is often unprepared to deal with these unexpected attacks. In this situation, AI systems usually require a lot of training time to update the model, but they cannot respond in time when an attack occurs, so the attack has already succeeded. Power network security maintenance personnel have to spend more effort and cost to continuously adjust and optimize AI algorithms to keep up with the pace of changing attacks, which also makes system security maintenance significantly more difficult and stressful.

(2) Potential risks to privacy protection and data security

The increasing reliance on data in power network systems has made privacy protection issues more complex. With the in-depth involvement of AI and data mining technologies, data has become a key but also a sensitive prized possession. Every small leak or abuse may lead to serious consequences. In power networks, AI technology often requires a large amount of user data to analyse and identify potential threats, which inevitably involves user privacy. However, there are still many loopholes in the existing technical means of privacy protection. On the one hand, the massive nature of data collection makes privacy protection meticulous and cumbersome. On the other hand, the lack of a sound protection mechanism may make user information irretrievable once it is leaked. More importantly, there is always a conflict between privacy protection and the efficiency of AI analysis, and it is conceivable how difficult it is to balance efficiency and security. The security of power networks is constantly testing the balance on the red line of protecting data security, but it is always difficult to find a foolproof solution.

(3) The unexplainability of the AI decision-making process has caused a crisis of user trust

The black box effect of artificial intelligence in the decision-making process gives people the feeling of looking at the flowers through the fog, causing users to have greater doubts about its safety and reliability. In an area with high security requirements such as the power grid, any decision made by AI is of great importance. Especially when facing critical security threats, the reasoning behind the AI decision is often shrouded in mystery and baffling. For some technical personnel, the inability to explain the logic behind a decision can raise significant doubts, and this also makes users defend themselves against AI. The opacity of the decision-making process makes many users worry about whether the system can really make the right judgment at critical moments. When the system needs to deal with unconventional threats, it is difficult for users to fully rely on AI decisions without trust. Therefore, the black box problem of AI decision-making has become the Achilles heel of power grid security, and the prospects for its application in the security field have also been overshadowed.

(4) The integration of traditional systems and new technologies is complex

It is difficult for the traditional power network system architecture and AI technology to integrate. Many of the hardware devices and infrastructure in power networks are often very old, and they were not even designed with AI in mind, making it difficult to achieve a perfect fit in terms of interface adaptation. There may be compatibility issues with every interface and every protocol, making integration a complex operation. To ensure that the AI system and the power network can work together smoothly, developers have to invest a lot of energy in system integration and compatibility testing, and each test may bring new problems. At the same time, the high cost of equipment upgrades and network debugging severely restricts the speed of adoption of new technologies, and may even affect the stability and safety of the entire system. Therefore, the separate administration of traditional systems and emerging technologies in the power network makes it difficult to achieve effective deployment, which also hinders the application of AI in the power network.

(5) High computing resource requirements limit real-time response capabilities

The advantage of AI technology is that it can process massive amounts of data, but its high demand for computing resources also makes real-time response in power networks difficult. Power networks require all-weather, all-round security monitoring, and any delay can pose a potential risk. AI often requires powerful computing power during operation, which poses a considerable challenge to the real-time nature of the system. AI algorithms consume a lot of resources when processing large amounts of data, making it difficult to respond quickly to attacks as they occur. This situation means that power networks may suffer damage before AI can respond to sudden attacks. Although technologies such as cloud computing can alleviate some of the pressure on resources, there is also a risk of delay in the coordination between the cloud and the power network. The high demand for computing resources limits the real-time monitoring capabilities of AI, making the security of the power grid inadequate in the face of emergencies. The conflict between resources and response capabilities has become an important bottleneck limiting the true value of AI.

4. System Construction Strategy Based on Artificial Intelligence and Data Mining Power Network Security

(1) Continuously update and optimise algorithms to respond to network changes

In order to effectively respond to the ever-changing network threats, continuously updating and optimising algorithms is a core task. This is not only the fundamental guarantee of the AI system's effectiveness, but also the cornerstone of power grid security. Currently, attack methods are not only changing with each passing day, but can even generate multiple variants in a short period of time, creating security risks in multiple dimensions. Therefore, AI models cannot rely on unchanging algorithms. A normalised update mechanism must be established to enable dynamic adjustment capabilities. The core of this mechanism is the ability to keenly identify new attack patterns and quickly adjust algorithm parameters, rather than just mending the fold to fix it. First of all, the continuity of the data flow is the foundation. Real-time data generated in the power network can be used, and automated data labeling and classification techniques can be used to ensure that the model always learns based on the latest threat scenarios[5]. Here, particular attention needs to be paid to capturing and defining abnormal behaviour. Small but abnormal behaviours can be collected in a database, so that pre-emptive protection can be carried out before the next attack occurs. To achieve this, it is recommended that companies introduce an adaptive learning model, combined with a real-time online monitoring platform, so that the model can learn and correct itself. This type of model can use repeated training and real-world training to make the best response in a shorter period of time.

To achieve truly efficient algorithm optimisation, continuous technological innovation and collaborative research and development are essential. It is recommended that a threat intelligence sharing mechanism be established within the security team, whereby internal technical personnel should maintain real-time information communication and share new threats and attack methods with each other, so as to improve the speed of identifying unknown threats. At the same time, in order to make optimisation more sustainable and forward-looking, a joint research and development mechanism should be established with external scientific research institutions and other power companies, combining multi-party data and cross-industry technical support to continuously innovate algorithms. For example, using Generative Adversarial Networks (GANs) or Transfer Learning to simulate diverse attack scenarios and generate similar but unique attack samples can improve the model's adaptability to mutated attacks. During the testing phase, it is recommended to adopt a layered testing plan: from offline simulation in a laboratory environment, to small-scale online testing, and then to full-system application, to ensure that the optimized model can not only operate effectively in an ideal environment, but also be able to remain unchanged in the face of change in a real and complex network. Finally, organise regular technical training and simulated attacks to train the team's response and collaboration skills in real combat, and ensure that the updated algorithms can be truly implemented in all aspects of network protection, forming an efficient system of rapid response and comprehensive protection.

(2) Strengthen privacy protection technology to ensure data security

In the power network system, strengthening privacy protection technology is not only a basic requirement for meeting compliance, but also a key measure to prevent the leakage of user information and maintain public trust. In the face of increasingly severe privacy and security risks, Differential Privacy technology has become the first choice. It introduces random noise to obscure personal information in the data set, making it difficult for attackers to identify individual information, even if overall trends are obtained from the data set. Specifically, it is recommended that Differential Privacy technology be embedded in all aspects of data collection and analysis, and that data be de-identified as soon as it is generated, so as to minimise the risk of leakage. For an area such as the power system that involves sensitive user information, it is recommended to apply local differential privacy. In this way, the data is encrypted at the user end to ensure that the information is de-identified before entering the system, which not only ensures the statistical value of the data, but also effectively isolates it from unauthorized access. At the same time, in data sharing and cooperation between different departments, the parameter settings for differential privacy should be strictly controlled to achieve the dual goal of sharing and security. In addition, an intelligent data audit system should be used to monitor the flow and use of data in real time, forming a closed-loop security control.

However, differential privacy is only part of privacy protection. To comprehensively protect data security, encryption technology is also needed to provide armour for data. In the actual operation and maintenance of power networks, the introduction of Attribute-Based Encryption (ABE) can be considered. Its characteristic is that access rights can be controlled based on user attributes (such as department, permissions, etc.). This encryption method can ensure that only users who meet specific conditions can decrypt the data, thereby further strengthening the security of the data during storage and transmission. For data in transit, it is possible to combine it with End-to-End Encryption technology, so that the data is encrypted as soon as it leaves the sender and remains sealed until it is decrypted at the receiver. In addition, the choice of encryption algorithm is also particularly important. It is recommended to regularly update the algorithm version to avoid security vulnerabilities caused by outdated algorithms. During the algorithm update process, a hierarchical encryption strategy can be adopted to encrypt data according to its importance and sensitivity to ensure multi-layer protection of core data. At the same time, in order to further enhance user trust, it is recommended that companies regularly publish transparent security reports to disclose the latest developments in privacy protection measures, and encourage users to participate in privacy feedback to form a comprehensive privacy security protection system with user participation.

(3) Improve the transparency and interpretability of decision-making

In the field of power grid cybersecurity, improving the transparency and interpretability of AI decisions is not just a technical choice, but the key to gaining user trust and ensuring the efficient operation of the system. The problem of uninterpretability in AI decisions is particularly prominent under the black box effect. Especially when dealing with sudden cybersecurity incidents, the judgments made by the system are often difficult to trace and understand, leading users to doubt the correctness of the decisions. Therefore, the first priority in improving transparency is to introduce Explainable AI (XAI) technology to ensure that the system can 'know not only what happened, but also why'. To achieve this effect, it is recommended to introduce the principle of transparency at the algorithm design stage, and to present the prediction and analysis results of each step of the model to the user in a structured manner, especially for professional operators in the security field. The use of such interpretable models allows AI to generate clear visual data and logical chains when making safety decisions, so that users can understand the reasoning process of the system at a conceptual level. In addition, local interpretation methods (such as LIME or SHAP) can be introduced to help technicians gain an in-depth understanding of which features and weights are used to make a specific decision, ensuring that there is a traceable path when further tracking and verification is required.

In order to build a transparent decision-making process, it is also necessary to strengthen the interactive feedback mechanism for users, so that the decision-making process of the system is not only transparent to professionals, but also provides appropriate explanations and feedback to a wider range of users. To this end, it is recommended to set up a decision explanation panel on the safety monitoring platform of the power network system, which displays in real time the factors and model parameters considered by the system when making a certain safety decision, so as to help users establish trust in each decision. At the same time, detailed decision-making records and historical analysis functions should be provided, so that users can retrieve the decision-making process within a specific time period as needed. This not only facilitates problem tracing, but also helps accumulate experience. Especially in the response to emergencies, being able to let users clearly know every step taken by the system and the model characteristics on which it is based not only improves the transparency of the system, but also enhances users' confidence in its operation. In addition, in the design of information feedback for system decisions, it is recommended to draw on the human-machine collaboration strategy, so that AI can actively prompt and consult with users before making key decisions, giving users the opportunity to participate in the decision-making process and strengthening their understanding of and trust in AI. By continuously optimising the explanatory function and strengthening the interactive feedback mechanism, the decision-making of AI systems will no longer be a show, but a means of safety assurance that users and technicians can jointly participate in and understand.

(4) Improve the system architecture and enhance technical compatibility

To effectively improve the technical compatibility of the power system, upgrading and transforming the system architecture has become an indispensable and crucial step. The traditional power system architecture is designed based on functional modularity and a closed operation concept, while AI technology emphasises open data integration and rapid response[6]. To achieve seamless integration of the two, adaptive adjustments need to be made at the system architecture level. The first step is to focus on building a standardised and modularised infrastructure, and comprehensively implement standard interfaces, from the interface to the data format. Microservices Architecture can be introduced. By breaking down the system into a series of service modules, each module communicates with each other through a unified standard API interface. In this way, during the updating and integration of the AI system, it is not necessary to make holistic modifications to the entire system, but only to make targeted adjustments to specific service modules. In addition, distributed processing methods such as Edge Computing can also be introduced into the hardware part of the traditional power system, moving some of the computing requirements closer to the edge of the network near the terminal, to reduce the delay caused by data transmission and thereby improve the real-time performance and adaptability of AI technology in the power system [7].

In addition, adaptability testing is crucial in the process of integrating AI and the power system. In the process of upgrading the architecture, the transition and integration of new and old technologies is inevitable. This not only requires technicians to fully understand the operating logic of traditional systems, but also requires detailed adaptability testing for compatibility issues. It is recommended to adopt a layered incremental testing approach, that is, gradually testing from subsystems to the overall network. First, the performance of different modules is tested in a simulated environment, and then it is applied in a small area in the actual operating environment, gradually expanding the coverage. This gentle integration approach can effectively avoid the risk of system instability caused by compatibility differences. In addition, power companies should consider establishing strategic partnerships with professional technology suppliers to enhance the compatibility of existing equipment with their technical support and upgrade services. To meet future expansion needs, open interfaces can be reserved to gradually form a system architecture that is flexibly adaptable and open and compatible. Such an architecture not only lays the foundation for the application of AI in power systems, but also helps the system maintain high stability and scalability during technological iteration.

(5) Optimise resource allocation and improve real-time response capabilities

In the process of improving the real-time response capabilities of the power system, optimising resource allocation is the key to achieving efficient operation. The real-time requirements of the power system determine that the deployment of AI technology not only requires sufficient computing resources, but also careful planning of the allocation and use of these resources. Currently, the computing power required by AI to process huge data sets often conflicts with the real-time monitoring requirements of power networks. To this end, resource layering and dynamic allocation strategies can be introduced [8]. For example, in terms of system architecture, high-priority tasks such as intrusion detection and critical early warning can be assigned to local servers with real-time computing capabilities. For low-priority tasks such as deep learning model training of historical data, they can be arranged in the cloud or in an off-site data centre to reduce the burden on core computing equipment. The advantage of this layered architecture is that it can ensure that mission-critical tasks are not affected by other operations, ensuring real-time performance of the system. During implementation, it is recommended to set up a resource scheduling strategy that dynamically monitors the resource consumption of each task module and makes real-time adjustments based on the urgency of the task and resource usage. This improves the efficiency of resource utilisation without increasing hardware investment.

Distributed computing and edge computing are also powerful means that should not be overlooked in terms of further optimising computing strategies. By transferring some data processing to edge nodes close to the data source, the burden on the core system can be reduced, which can greatly shorten the data transmission delay and enable the AI system to make safer decisions more quickly. Distributed computing can break down tasks into different computing nodes for parallel processing, which can significantly improve computing speed and task processing flexibility, especially when dealing with large amounts of data. In addition, to improve the stability of real-time responses, power companies can consider deploying an Elastic Computing architecture, which automatically scales computing resources up or down according to demand to cope with high load fluctuations and ensure the adequacy of system resources at critical moments. It is recommended that the operating status of each node be monitored and optimised on a regular basis to identify resource bottlenecks and adjust configurations in a timely manner. This multi-faceted resource optimisation solution not only improves the system's response speed, but also ensures that AI technology can provide safety and security in the best possible condition during emergencies.

5. Conclusion

In summary, despite the inevitable contradictions, compared with the traditional electric power network system, the security of electric power network with the addition of new science and technology such as artificial intelligence and data mining has been significantly improved, and the prospects for the use of artificial intelligence and data mining and other emerging technologies in the network security of electric power system are still quite promising. In the future, with the continuous development of information technology, as well as the continuous optimization of the power network system, a large number of more outstanding professionals, I believe that artificial intelligence and data mining technology in power network security research will have a greater breakthrough.

References

[1] Wan Jianghong. A data mining-based approach for recognizing the security posture of electric power communication networks[J]. Changjiang Information and Communication, 2024, 37 (04): 98-100.

[2] Bai Bing, Duan Xiaochen. Research and realization of power network security alarm information mining[J]. Automation and Instrumentation, 2023, (05): 87-91.

[3] LIU Cuijuan, HENG Junshan, CHANG Jingwei. Application of intrusion detection system based on data mining and rough set in electric power network[J]. Journal of Chengde Petroleum College, 2008, (01): 30-33.

[4] Ying Jieyao. Research progress on smart grid data security issues based on Internet of Things technology[J]. Electronic Science and Technology, 2023, 36 (03): 76-80.

[5] Gao Xiang, Chen Guifeng, Zhao Honglei. Cyber security posture assessment of electric power information system based on data mining[J]. Electrical Measurement and Instrumentation, 2019, 56 (19): 102-106.