Exploration of Computer Network Security Issues under Internet of Things Technology

Haikang Gu
Lanzhou Bowen College of Science and Technology, Lanzhou 730100, China

Abstract: With the continuous improvement of social development level, computer network technology has achieved deeper application and popularization in various fields, promoting the vigorous development of various industries. However, while computer networks provide convenience for people's lives, there are also certain security risks. To ensure the secure and stable operation of the computer network system, this article will discuss the security issues of computer networks under the Internet of Things technology and propose some measures for reference only.

Keywords: Internet of Things technology; Computer network security; Problem

Introduction: With the continuous development of IoT technology, it also provides new technical support for computer network security protection work. In the process of analyzing computer network security, staff should actively introduce relevant means of Internet of Things technology, so as to significantly improve the efficiency and quality of computer network security management, create a more complete network security mechanism, ensure the smooth operation of the computer network security system, and meet people's growing network security needs.

I. Internet of Things Technology and Application Analysis

At present, there is no consensus on the definition of the Internet of Things. Based on historical experience analysis, we can summarize and generalize the definition of Internet of Things technology, which can be summarized into two aspects. One is the interconnection relationship between physical objects built based on the Internet of Things, in order to extend the network coverage area. Another approach is to use computer communication technology, IoT identification technology, intelligent perception technology, etc. to build a bridge for the exchange of item information. In practical applications of physical networks, it is necessary to combine them with mobile communication technology and deploy sensing devices in various fields to achieve more comprehensive and detailed control and improve people's work efficiency. Based on the analysis of domestic and international forms, cyber attacks have become a globally ranked risk and a significant risk factor that cannot be ignored. With the continuous development of computer technology, computer network issues have received increasing attention, and network security has become an important issue for competition among countries. Therefore, we should conduct in-depth research on computer network security issues under the Internet of Things technology, laying a solid foundation for improving the level of computer network security.

II. Computer Network Security Issues under Internet of Things Technology

1. Security issues of terminal nodes

Due to the fact that network terminal devices usually operate in an unsupervised environment, many terminal links lack effective control, which can significantly reduce their security level. The main problems faced by terminal nodes are threefold, one of which is the serious situation of unauthorized use. Due to the lack of effective monitoring of the usage rights of terminal devices, they are easily vulnerable to illegal attacks and intrusions. If they are invaded by the network, attackers can freely modify data information, resulting in serious impacts. The second possibility is the risk of node information leakage. Malicious attackers may cause network terminals to be compromised, resulting in the leakage of confidential information, which in turn can give attackers access to data and pose a threat to information security. The third issue is the problem of malicious impersonation of perception nodes. Invaders can use technological means to impersonate perception nodes, injecting false information into the network and launching malicious attacks, such as publishing false messages, seriously disrupting the secure operation of the network.

2. Communication security issues

If the proficiency of communication terminals is insufficient or the information carrying capacity of the network is not high, it can lead to serious external threats to the computer's intranet, and even network congestion may occur. The Internet of Things integrates a large number of devices, and if the current device authentication mechanism is adopted, it will generate a large amount of information traffic. When multiple devices make network requests simultaneously, it can have a serious impact on the overall network. The current network communication generally adopts a one by one authentication method, which can improve the level of key security. However, IoT devices also need to access corresponding keys, which invisibly occupies certain network resources. As the types of IoT services become increasingly diverse, when the same user uses the same device and the number of authentication increases, it can lead to key accumulation, thereby consuming network resources.

3. Perception layer security issues

In the perception layer, if RFID tags or smart devices invade items without authorization, they will illegally obtain the owner's location

information and other content, greatly infringing on personal privacy. During this period, RFID tags may issue some unauthorized requests, which can pose certain security risks to positioning, tracking, etc. IoT terminal devices typically operate in unmanned areas, which increases their risk of being attacked. Attackers can modify or replace terminal software and hardware, leading to security issues with perception nodes.

III. Computer Network Security Measures under Internet of Things Technology

1. Adopting encryption mechanisms in the Internet of Things

At present, China's level of informatization is constantly improving, and network problems are becoming increasingly apparent, which are related to many aspects such as trade secrets, personal privacy, and national information security. In order to ensure the continuous improvement of computer network security, we can try to use advanced encryption mechanisms with the help of IoT technology, which can penetrate deep into the network layer and provide more comprehensive and diversified encryption protection for data transmission. Moreover, the clause by clause encryption mechanism can further expand the application scope of IoT technology, thereby better adapting to the high security requirements of IoT.

Under the protection of item by item encryption mechanism, information will be added with multiple layers of protection during transmission, and then exist in the form of passwords and ciphertexts, which can greatly enhance the security of information. The ICC in the Internet of Things plays a key role in connecting and serving businesses. By developing a more standardized format for text information during the flow and reception of information, the difficulty of deciphering information can be greatly increased, thereby significantly enhancing the security of network information transmission. It is worth noting that the implementation cost of each encryption mechanism is relatively low and time-consuming, which can significantly improve the overall level of network security, and this also gives it a very broad development prospect. In practical operation, item by item encryption is not an unconditional encryption process for all transmitted information, but rather for some valuable, highly private, and secure information. Through this processing method, the encryption workload of technical personnel can be greatly reduced, thereby ensuring high security in the use of the Internet of Things. By introducing item by item encryption mechanisms into practical work, the comprehensive level of computer network security can be greatly improved. In addition to creating a more secure network environment, it can also provide corresponding technical support for the long-term and healthy development of IoT technology.

2. Use secure routing

The Internet of Things itself is a relatively complex network system, mainly composed of two core parts: the communication layer and the perception layer. In this system, each device can collect corresponding information through the perception layer, and then transmit this information through the communication layer, which involves the routing problem of the Internet of Things. The selection and design of routing can have a significant impact on the efficiency and security level of information transmission. Therefore, when carrying out routing design for the Internet of Things, it is necessary to consider different network systems, which can greatly improve the efficiency of information transmission. To further enhance the security of routing networks, we can analyze two issues.

One is the issue of routing security in multi network environments. In a multi network environment, the design of routing requires the formation of similar information between identity tags and IP addresses, in order to create a unified routing architecture. This can greatly improve the traceability and recognition level of routing, thereby enhancing the security of routing.

The second issue is the routing security of sensor networks. Due to the limited resources of sensors, such as their storage capacity, energy, computing power, etc., they are more vulnerable to external network attacks. Therefore, when designing routing for sensor networks, it is possible to introduce more secure routing algorithms to better resist network attacks such as denial of service and tampering with services. At the same time, we also need to carry out more reasonable configuration of sensors to enable them to complete routing tasks more efficiently with limited resources. Overall, the routing problem of the Internet of Things is a very complex and important research topic. Staff can start with routing security at multiple network environments, sensor networks, and other levels, and use advanced algorithms and computer technology to significantly improve the level of computer network security under the Internet of Things.

3. Perform position detection effectively

In order to better reduce the risk of unauthorized use of the Internet of Things, technicians can adopt the strategy of establishing a dedicated network monitoring platform to deal with it, which can greatly improve the management ability of IoT terminals. When performing corresponding network monitoring tasks, we can carefully monitor the terminal devices and their locations to obtain detailed information about the corresponding targets, and the terminal devices can passively report their locations. Staff can use network infrastructure such as MME to receive corresponding information content and then upload it to the server. After receiving the corresponding location information, the server can conduct a more comprehensive analysis and judgment of the content of this information. If there is a discrepancy between the analysis results and the location information, it indicates that the terminal device may have left the authorized area. In this case, the network infrastructure can send corresponding alert information to the server. After receiving the alarm information, the server can re verify and process the location of the terminal device to ensure its legality. For some devices with poor mobility, if there is a change in location, the monitoring system can quickly detect and issue warnings to prevent illegal device movement in a timely manner, which can greatly improve the security and reliability of information.

4. Strengthen the application of firewall and intrusion detection technology

To further enhance the security level of information transmission in the Internet of Things, we should analyze the essential characteristics of computer networks and understand their operating mechanisms. By analyzing this knowledge, a more reasonable and scientific firewall system can be created, which can effectively adapt to different network environments and better meet the actual needs of users. By designing access control mechanisms, it is possible to achieve isolated management of different networks, thereby significantly improving the security level of the entire network. After the network is effectively isolated, each independent network can enjoy a higher level of security when performing information transmission tasks. This not only means a significant improvement in data transmission security, reducing the probability of attackers tampering and stealing information, but also effectively ensuring data integrity and effectiveness, allowing information to be utilized in a secure environment.

Technicians can use monitoring technology to detect and handle intrusion behavior at the application layer of the network, which can significantly improve response and processing efficiency, further enhancing the level of computer network security. When facing different types of intrusion threats, technicians can adopt appropriate strategies to carry out vulnerability repairs and ensure the stability of network defense. In addition, we can use quantitative and qualitative analysis methods to conduct more in-depth research on conventional and unconventional intrusions, in order to reduce the impact of intrusion behavior on network security and ensure work stability.

Epilogue

In the process of strengthening the construction of computer network security system, in-depth exploration of IoT technology is particularly crucial. As an important technological support, IoT technology provides a solid guarantee for computer network security prevention and effectively promotes the optimization and improvement of the computer network security system. This article focuses on computer network security issues from the perspective of the Internet of Things, and conducts in-depth analysis from multiple dimensions, aiming to promote the innovative development and systematic construction of computer network security work in China.

Reference:

[1] Bo Song. Research on Network Security Issues and Response Strategies Based on Internet of Things Technology [J]. Network Security Technology and Applications, 2023 (09): 160-161.

[2] Chao Jin. Analysis of Internet of Things Computer Network Security and Remote Control Technology [J]. Electronic Technology and Software Engineering, 2023 (06): 25-28.

[3] Jiang Wu. Application Analysis of Internet of Things Technology in Network Security [J]. Information and Computer (Theoretical Edition), 2022, 34 (05): 200-203.

[4] Jianglong Guo. Research on Computer Network Security Issues and Response Strategies Based on Internet of Things Technology [J]. Public Standardization, 2022 (01): 61-63.

[5] Changqing Ye. Network Security Issues and Countermeasures Based on Internet of Things Technology [J]. Science and Technology Information, 2021, 19 (32): 14-16.

[6] Yangping Chen. Network Security Issues and Countermeasures Based on IoT Technology [J]. Network Security Technology and Applications, 2021 (10): 11-13.

[7] Yousong Zhang. Internet of Things Computer Network Security and Remote Control Technology [J]. Computer Knowledge and Technology, 2021,17 (26): 28-29+44.