

# Application of Internet of Things Technology in Computer Network Security and Remote-Control Analysis

Shouning Huang, Guangxi Technological College of Machinery and Electricity, China\*

## ABSTRACT

Internet of things computer network technology can not only speed up the information transmission, but also help to break the previous time and space restrictions and improve the actual work efficiency. However, in the practical application and development of this technology, the realization of data security technology and remote control technology is the key to improve its application effect and ensure data security. Due to the obvious openness of the internet of things computer network itself, common security risks emerge one after another. Therefore, in practical application, it is necessary to pay more attention to security management and maintain network security.

## KEYWORDS

Computer, Internet of Things Technology, Network Security, Remote Control

## INTRODUCTION

With the increasing level of computer network applications, the factors affecting computer network security are also increasing. Various network crises such as personal privacy exposure, network virus invasion, system vulnerability, hacking and other serious threats have become a great concern in the world (Aggarwal et al., 2020). The Internet of Things (IoT), as the third wave of the world's information industry after computers and the Internet (Aldaej, 2019), has also made rapid progress against the backdrop of the growing technological level in China.

IoT technology enables the establishment of interconnected channels among objects via networks. In terms of its components, IoT is characterized by a layered structure that distinguishes different functionalities. For instance, the application layer is responsible for processing relevant data and information, as well as making final decisions based on them. (Al-Sibai et al., 2021). The network perception layer needs to acquire the state of objects according to the tasks corresponding to its own operational functions, and the tasks of the information network layer need to transmit information in an orderly manner and collect the corresponding data. IoT technology and remote-control technology are integrated into the IoT smart home, and wireless technology is used to speed up the transmission of information. The IoT serves as a carrier for basic data connectivity and realizes the mutual integration

DOI: 10.4018/IJWSR.342120

\*Corresponding Author

This article published as an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

between things and networks. Through remote control technology, the internet is used to effectively control remote devices and ensure the secure operation of computer networks. However, as IoT devices continue to expand, network security issues become more complex and critical. Securing the IoT, especially in terms of data transmission and device authentication, becomes particularly important (Sitaraman, 2022). In response to these challenges, further research and development of secure and reliable routing mechanisms, device authentication mechanisms, and the like are needed to ensure the security and stability of IoT systems (Chatfield & Reddick, 2019).

The rapid development of the IoT brings great convenience to people's lives and privacy issues. Therefore, it becomes crucial to construct a secure and reliable privacy protection mechanism (Dovhan et al., 2019).

The objective of this thesis is to explore the development of a resilient privacy protection mechanism within the IoT technology environment. The study begins by examining the utilization of digital signature techniques for encrypting network data, thereby ensuring its confidentiality and integrity. Additionally, focus is placed on employing various security techniques, including encryption, firewalls, intrusion detection, and prevention systems, to safeguard network security against the growing sophistication of cyber threats.

In the IoT environment, we further explore the design and implementation of secure routing mechanisms. By rationally planning the network topology, optimizing routing algorithms and introducing fault recovery mechanisms, we aim to improve the robustness and reliability of IoT systems.

In addition, we will study techniques in authentication and remote control to ensure that only authorized users can access and operate IoT devices.

By conducting detailed validation experiments and performance analysis, the feasibility and effectiveness of the proposed mechanisms will be evaluated. The research aims to offer substantial evidence supporting the construction of a secure and reliable privacy protection mechanism, thereby fostering the sustainable development of IoT technology.

## **RELATED WORKS**

Li (2013) presents the implementation details of the protocol. As people pay more attention to the security of network communication, in order to improve the security of computer network communication, the application of data encryption technology has become an important technical means (Li, 2013). Based on Zhang (2018), we make an in-depth analysis on the application of data encryption technology in computer network communication security. With the expansion of the current application of big data technology, the application in computer network information security has gradually developed, which has a positive effect on improving computer network information security and protection benefits. Chu et al. (2021) conduct analysis of network security and privacy security based on AI in the IoT environment. The network security risks caused by AI and IoT applications are analyzed in Chu study. In the application of computer network communication security technology, the application of data encryption technology is to ensure people's privacy and security. Chen makes a preliminary analysis and discussion on the problems of computer network management and information security prevention (2021). Data is the basis of information technology security management, and with the arrival of the era of big data, computer network security also faces many challenges. The network has open and virtual characteristics, which present many security risks (He, 2021). He (2021) explores the main hidden network security danger and puts forward the corresponding precautions to the computer information network security precautions. The information age Internet technology is widely used, but computer network security problems also often appear, often a variety of viruses invade the computer, so He strengthen the network security management, and put forward countermeasures, so as to improve the level of network security, strengthen network security protection, is very important (He, 2021) .

16 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: [www.igi-global.com/article/application-of-internet-of-things-technology-in-computer-network-security-and-remote-control-analysis/342120](http://www.igi-global.com/article/application-of-internet-of-things-technology-in-computer-network-security-and-remote-control-analysis/342120)

## Related Content

---

### Karma2: Provenance Management for Data-Driven Workflows

Yogesh L. Simmhan, Beth Plale and Dennis Gannon (2008). *International Journal of Web Services Research* (pp. 1-22).

[www.irma-international.org/article/karma2-provenance-management-data-driven/3117](http://www.irma-international.org/article/karma2-provenance-management-data-driven/3117)

### Leveraging Incrementally Enriched Domain Knowledge to Enhance Service Categorization

Jia Zhang, Jian Wang, Patrick Hung, Zheng Li, Neng Zhang and Keqing He (2012). *International Journal of Web Services Research* (pp. 43-66).

[www.irma-international.org/article/leveraging-incrementally-enriched-domain-knowledge/74706](http://www.irma-international.org/article/leveraging-incrementally-enriched-domain-knowledge/74706)

### Security and Privacy Issues of Big Data

José Moura and Carlos Serrão (2019). *Web Services: Concepts, Methodologies, Tools, and Applications* (pp. 2197-2229).

[www.irma-international.org/chapter/security-and-privacy-issues-of-big-data/217939](http://www.irma-international.org/chapter/security-and-privacy-issues-of-big-data/217939)

### Importance and Usability of University Websites

Ersin Caglar (2022). *App and Website Accessibility Developments and Compliance Strategies* (pp. 1-37).

[www.irma-international.org/chapter/importance-and-usability-of-university-websites/287252](http://www.irma-international.org/chapter/importance-and-usability-of-university-websites/287252)

### Behavioral Attestation for Web Services Based Business Processes

Masoom Alam, Mohammad Nauman, Xinwen Zhang, Tamleek Ali, Patrick Hung and Quratulain Alam (2012). *Web Service Composition and New Frameworks in Designing Semantics: Innovations* (pp. 308-329).

[www.irma-international.org/chapter/behavioral-attestation-web-services-based/66965](http://www.irma-international.org/chapter/behavioral-attestation-web-services-based/66965)