Application of Virtual Network Technology in Computer Network Security (Postprint)

Authors: Song Lingmei

Date: 2023-10-08T00:00:00+00:00

Abstract

Since the 21st century, the penetration rate of computers and the Internet in our country has continuously increased, with computer and Internet technology permeating every aspect of public production and life, becoming one of the essential tools for social life and production. "Science and technology are a double-edged sword." While computer networks have created a diversified, interactive information circulation space for the public, they have also brought about numerous problems, among which computer network security issues are particularly prominent. For instance, information leakage caused by improper personal operation or weak security awareness, and hacker attacks resulting from inadequate security measures, all threaten the public' s information and property security. Therefore, it is imperative to apply advanced virtual network technology to enhance computer network security and provide computer network users with high-quality, secure services for information dissemination, storage, and content. This article begins with the characteristics and types of virtual network technology, designing a computer network security system centered on virtual network technologies such as cloud computing, encryption keys, and data encryption, aiming to provide ideas for computer network security management and protection.

Full Text

Preamble

Application of Virtual Network Technology in Computer Network Security

(Office of Cybersecurity and Informatization Committee of Manas County, CPC, Changji Prefecture, Xinjiang 832200)

Abstract: Since the 21st century, the proliferation of computers and internet technology in China has penetrated every aspect of public production and daily

life, becoming an indispensable tool for social activities. However, "science and technology are a double-edged sword." While computer networks have created diversified, interactive information exchange spaces for the public, they have also introduced numerous problems, with cybersecurity issues being particularly prominent. Problems such as information leakage caused by improper personal operation or weak security awareness, and hacker attacks resulting from inadequate security measures, constantly threaten public information and property security. Therefore, there is an urgent need to apply advanced virtual network technology to enhance computer network security and provide users with high-quality, secure services for information transmission, storage, and content. This article begins by examining the characteristics and types of virtual network technology, then designs a computer network security system centered on cloud computing, encryption, and data encryption technologies, aiming to provide insights for network security management and protection.

Keywords: virtual network technology; characteristics and types; computer; network security; system design
Classification: TP393
Document Code: A
Article ID: 1671-0134(2021)02-105-03
DOI: 10.19483/j.cnki.11-4653/n.2021.02.031
Citation Format: Song Lingmei. Application of Virtual Network Technology in Computer Network Security[J]. China Media Technology, 2021(02):105-107.

Virtual network technology has opened new dimensions for network services, enabling users to access and utilize massive network resources anytime and anywhere, while breaking through geographical and temporal constraints to perform data storage, expansion, and other operations on corresponding terminals. However, against this backdrop, computer network security issues have also taken on new forms and characteristics. Network viruses, hacker attacks, and other threats exploit security vulnerabilities to steal, tamper with, or illegally use data on personal computers, posing serious threats to user information and property security. Traditional network security management approaches store data on dedicated servers, requiring users to access information through regional networks and servers. While this approach offers some data protection, extracting data from storage servers creates time lags that reduce data accuracy and timeliness. In contrast, computer network security management systems based on virtual network technology offer advantages such as strong scalability and continuous availability. By integrating distributed data into a centrally managed data center, these systems can effectively separate servers from stored data while maximizing user data security. The following sections briefly explain the characteristics and types of virtual network technology, focusing on analyzing application strategies for enhancing computer network security.

1.1 Characteristics of Virtual Network Technology

A virtual network refers to a computer network that contains virtual links—in other words, data transmission between two computing devices occurs not through physical connections like network cables, but via network virtualization. Virtual network technology transforms public network areas into specific network usage zones to build private networks, then employs data encryption, identity authentication, and other methods to protect computer network security. As an important component of network technology, virtual network technology not only enhances computer network security but also helps create more stable and functionally diverse network environments. It effectively addresses cybersecurity issues by largely preventing data transmission distortion, defending against virus and hacker attacks, and reducing the probability of data loss, damage, or theft. Additionally, virtual network technology provides users with higher-quality services for network storage, transmission, preservation, and expansion, facilitating both daily life and work.

Virtual network technology features simple structure and low application costs. First, it can improve existing network structures by eliminating redundant components, thereby enhancing the quality and efficiency of network security management and maintenance. Second, by reducing physical connections between devices, it lowers the cost of network construction.

1.2 Types of Virtual Network Technology

Virtual network technology typically includes three major types: encryption technology, identity authentication technology, and key encryption technology.

Encryption technology is commonly used in computer network security. Its principle involves transforming data in public networks into encrypted form based on specific algorithms and data manipulation methods, which is then decrypted back into ordinary data when transmitted to the user' s system. This widely applied technology ensures data transmission security and confidentiality while largely preventing data distortion, making it highly valuable.

Identity authentication technology operates on the principle that users create dedicated, independent accounts within the network' s information repository, complete with usernames and strong passwords. Users upload their initial information through these specialized accounts, which serves as dynamic instructions for future data operations. During data transmission, devices perform real-time comparisons between internal and initial data to continuously authenticate the user' s identity, thereby ensuring data transmission security.

Key encryption technology generally includes two types: private key and public key. In private key encryption mechanisms, data is encrypted using a secret key shared between sender and receiver, based on the premise that the key has been exchanged manually without compromising network security. In public key encryption mechanisms, each user possesses two keys: one privately retained (the

private key) and another placed in the public network area. When an information sender wants to transmit data to a user, they encrypt the information using the public key, and the user decrypts it using their private key upon receipt.

2. Application of Virtual Network Technology in Computer Network Security

In the highly informatized era, the density and speed of information propagation in computer networks have reached unprecedented levels. Addressing how to process massive data volumes while ensuring secure data transformation, transmission, and storage has become an urgent challenge in building network security systems. Cloud computing, as a fusion of distributed computing, parallel computing, network storage, and virtualization technologies, can process tens of thousands of data points within seconds. Combined with its characteristics of virtualization, dynamic scalability, on-demand deployment, and high flexibility, it has become an indispensable network application concept in computer network security services. This section designs a computer network security system within a cloud computing environment, utilizing encryption and key encryption virtual network technologies.

2.1 Design Philosophy for Computer Network Security System Based on Virtual Network Technology

Any computer network security system design must center on user requirements. In cloud computing environments, users demand higher performance for data transmission, storage, extraction, and application, while also expecting functions such as automatic vulnerability repair and intelligent security risk identification. Consequently, they have more diverse requirements for network security performance. Cloud computing is not merely a network technology but a new paradigm of network application and service thinking aimed at building cloud data centers with interconnected and shared data resources. Therefore, designing network security systems in cloud computing environments requires not only correct, flexible, and rational use of cloud computing technology but also application of its distributed and centralized processing concepts. Currently, most computer network security systems in China still employ traditional server-based data storage models. With increasing data transmission and storage volumes, system function expansion, and diversified user requirements, such systems have become inadequate, showing significant lag and limitations.

To address this, the computer network security system designed in this article integrates virtual network technology, network security technology, computer technology, and data storage technology, placing data storage and management in separate processes to avoid mutual interference between system modules and maintain operational stability. Simultaneously, it uses virtual network technology to collect, process, and feed back system operation data, effectively identifying potential network security risks and preventing damage to user information

and property.

2.2.1 Cloud Architecture Design for Computer Network Security System

Effective application of virtual network technology in computer network security systems requires creating specific environments and conditions. The designed cloud architecture must possess two key characteristics: first, intelligent features. The system must have self-governance capabilities to respond intelligently to cloud platform requirements, necessitating embedded automation technology. Second, agility features. The system must respond quickly to changes or demand signals and adjust rapidly as system requirements evolve, requiring embedded virtualization technology.

The cloud architecture for the computer network security system based on network technology includes two main modules: a network packet processing module, which processes network packets in software form and extracts transmitted data through TCP reassembly and iSCSI protocol parsing; and a data encryption/decryption module, which performs data encryption and decryption in hardware form. To ensure effective connection between these two module processes, shared memory is used for data transmission, allowing dynamic adjustment of CPU allocation. For instance, if the network packet processing module executes slowly, its CPU allocation ratio is increased. Additionally, the MiCA encryption/decryption engine is used to implement secure system networking.

2.2.2 Overall Functional Design of Computer Network Security System

The designed computer network security system operates as a transparent encryption/decryption gateway. Since it may handle massive data transmission and storage simultaneously, it must maximize system stability while preventing data damage and loss. The most common method for reducing inter-module coupling and improving overall system stability and disaster recovery capability is separating the control plane from the data plane. Under this approach, the system is highly modular, and a failure in one module does not affect the execution of other modules. The system hardware platform uses the Tilera Gx36 chip, consisting of 36 CPUs and peripherals, which are divided into control plane CPUs and data plane CPUs.

Given that different users have varying requirements for network security systems, multiple system functions must be designed accordingly. First, comprehensive security assessment of the network security system based on virtual network technology. Second, identification and discovery of potential system risks. Based on these foundations, the system' s overall functions include three main aspects: first, secure storage, encrypted transmission, decryption processing, and encrypted storage for user login and registration. Second, digital certificate generation, allowing users to independently select files for encryption and

store them following the aforementioned process. Third, data operation functions, requiring user verification before information extraction and subsequent encrypted transmission to the client.

2.2.3 Functional Module Design of Computer Network Security System

Based on the cloud architecture and overall functions described above, this section analyzes the design of control plane and data plane communication functions, network packet processing module functions, and data encryption/decryption module functions.

First, control plane and data plane communication function design. The control plane CPU leverages the bidirectional data transmission mechanism between kernel mode and user mode inherent in Linux systems to achieve high-speed packet forwarding. The data plane CPU runs on the ZOL core. Communication between the two occurs through shared memory and sockets. The data plane feeds back system operation parameters to the control plane, enabling intelligent perception of system status, while the control plane provides initialization data and configuration management for the data plane.

Second, network packet processing module function design. This module' s functions include two aspects: extracting transmitted data from packets received at network ports, and restoring data processed by the encryption/decryption module to its original packet format. Specific functions primarily include TCP flow reassembly, iSCSI protocol parsing, data splitting, and packet reconstruction.

Third, data encryption/decryption module function design. Due to the large volume of data transmission and storage in this system per unit time, software-based 3DES algorithm is adopted for data encryption and decryption.

The network packet module and data encryption/decryption module selected in this article operate synchronously as two process groups, with inter-process communication based on shared memory using a linked list queue data structure. New nodes generated by the network packet module are added to the end of the linked list queue, while the encryption/decryption module extracts nodes from the head for processing. The linked list queue in shared memory is shown in Figure 1 [Figure 1: see original paper].

The system' s data encryption/decryption module implements functionality using the 3DES algorithm, which is more difficult to crack than DES and enhances algorithm security through key mapping mechanisms. The encryption/decryption principle based on 3DES algorithm is shown in Figure 2 [Figure 2: see original paper], and the key mapping relationship is shown in Figure 3 [Figure 3: see original paper].

Computer network security management and prevention constitute a systematic, complex, long-term, and continuous undertaking. Especially in cloud computing environments, personal computer networks can flexibly access various types

of networks through network virtualization. If security protection measures are inadequate, account passwords are poorly protected, or personal operations are improper, these factors may create opportunities for hackers, viruses, and malicious actors to infiltrate. Therefore, appropriate virtual network technologies are urgently needed to solve network security problems, prevent data transmission distortion, protect user privacy, and safeguard information and property, thereby effectively enhancing computer network security.

The computer network security system designed in this article is based on a cloud computing environment primarily because, with technological development and increasing internet penetration, users' demands for network system functions and security continue to grow, requiring the ability to transmit and receive massive amounts of information within short timeframes. Traditional network application and processing concepts can no longer meet users' diversified needs. Meanwhile, cloud computing has evolved beyond a distributed computing method into an integration of distributed computing, network storage, and virtualization technologies, offering broad development prospects. This article designs a computer network security system based on the cloud computing environment, utilizing encryption, key encryption, and digital authentication virtual network technologies to enable massive data transmission, storage, and expansion while ensuring user data security, demonstrating high practical value.

Although virtual network technology offers significant advantages over other network technologies, its application in computer network security remains at a relatively basic level due to the special nature of network security and insufficient application experience. Therefore, further research and development efforts are needed to apply virtual network technology to all aspects of network security while adhering to the principle of balancing technical and economic considerations, thereby promoting the universal and widespread development of virtual network technology.

References

[1] Duan Cuihua. Application of Virtual Network Technology in Computer Network Security[J]. Network Security Technology and Application, 2021(01):8-9.
[2] Zhang Cunye. Analysis of the Role and Effect of Virtual Network Technology in Computer Network Security[J]. Computer Programming Skills and Maintenance, 2020(12):144-146.
[3] Lan Fangli. Application of Virtual Network Technology in Computer Network Security[J]. Network Security Technology and Application, 2020(12):28-29.
[4] Jiang Dacong. Application and Discussion of Virtual Network Technology in Computer Network Security[J]. Computer Knowledge and Technology, 2020, 16(30):30-31.
[5] Tong Ying, Zhou Yu, Yao Huanzhang, Liang Jian. Analysis of Application Value of Virtual Network Technology in Computer Network Security[J]. China New Communications, 2020, 22(20).
[6] Du Yu. Application of Virtual Private Network Technology in Computer

Network Information Security[J]. Electronic Technology and Software Engineering, 2020(20):237-238.
[7] Yin Haole, Zheng Zhihua, Yang Xiangyi. Practice of Virtual Private Network Technology in Computer Network Information Security[J]. Electronic Technology and Software Engineering, 2020(20).
[8] Hong Xiaojian. Application of Virtual Network Technology in Computer Network Security[J]. Network Security Technology and Application, 2020(10):41-43.
[9] Wang Ke. Discussion on Computer Network Security Prevention Measures in the Big Data Era[J]. Information and Computer (Theoretical Edition), 2020, 32(18):211-212.

Author Biography: Song Lingmei (1972-), female, from Jingjiang, Jiangsu, senior engineer, engaged in network security work, research interests: network security, network transmission, data security, etc.
(Responsible Editor: Yang Hu)

Note: Figure translations are in progress. See original paper for figures.