INTERNATIONAL MULTI DISCIPLINARY JOURNAL FOR RESEARCH & DEVELOPMENT
eISSN 2394-6334 Impact factor: 8.854 Volume 13, issue 04 (2026)

COMPUTER NETWORKS AND THEIR SECURITY

Mr. Dandu Jayabharath Reddy
Assistant Professor, Bachelor of Science in Information Technology,
Sambhram University, Jizzax, Uzbekistan,
Email ID: bharath55.edu@gmail.com
Bolbekova Muhlisa
BS-IT Student, Sambhram University, Jizzax, Uzbekistan.
Email ID: mbolbekova2@gmail.com
Anvarova Farangiz
BS-IT Student, Sambhram University, Jizzax, Uzbekistan.
Kamolova Sevara
BS-IT Student, Sambhram University, Jizzax, Uzbekistan.

Abstract: This article provides a detailed analysis of modern methodologies and technologies for ensuring network security. The main security elements of our research are cryptographic methods, network monitoring systems (IDS/IPS), VPN technologies, and security policies. This article examines the effectiveness and existing weaknesses of each technology. Cryptographic methods, such as AES and RSA algorithms, play an important role in protecting the network, but due to some threats and attacks, their effectiveness decreases over time. Although IDS/IPS systems are effective in detecting dangerous actions in the network, their high efficiency requires constant updating of the system. VPN technologies increase network security, but their use by some services without sufficient data encryption can pose a risk. The article emphasizes the importance of developing and implementing effective methodologies for ensuring network security.

Keywords: network security, cryptography, AES, RSA, IDS, IPS, VPN, network attacks, DDoS, network monitoring, technologies and risks.

Introduction

Computer networks are an integral part of modern information technologies and serve as the basis for the development of innovative developments and services in various fields. Nowadays, computer networks play an important role not only for organizations and companies, but also for individual users. The widespread use of network technologies and the growth of the Internet require not only increasing the efficiency of information exchange, but also ensuring the management and use of network resources. When it comes to the security of computer networks, the first thing that comes to mind is the need to ensure the integrity, confidentiality and availability of the system. Confidentiality means ensuring that only authorized users have access to information. Network security systems identify various risks and threats and take the necessary measures to ensure the operation of the system. However, the complexities and new threats that arise in ensuring network security require the constant development of this area. Threats such as data theft, malware penetration into systems, and network analytics failures pose a risk of system failure, financial losses, and the loss of users' personal data by malicious individuals. Security threats are becoming increasingly complex, and the number of malicious programs (viruses, Trojans, rootkits, etc.) and attacks is increasing. At the same time, it is necessary to create effective means of protecting systems on the Internet and look for new ways to combat emerging threats. When protecting data using cryptography, it is encrypted and decrypted only by authorized users. Network traffic monitoring systems monitor all data flows on the network and help identify malicious actions. On the other hand, technologies such as

intrusion detection systems (IDS) and network protection systems (IPS) are used to detect malware and protect the network. These systems detect unknown attacks on the network, dangerous actions taking place on the network, and take countermeasures. VPN (Virtual Private Network) technologies can also be used to create secure network tunnels and restrict access to Internet traffic to authorized users.

Applications of Secure Network Methodologies

During the transmission of information, eavesdropping and modification attacks can be used to listen to, modify, and intercept information without the user noticing it during telephone communication lines, instant messaging over the Internet, video conferencing, and fax transmissions. The software that implements the attack easily converts digital sound in the CODEC (converting an analog video or audio signal to a digital signal and vice versa) standard into high-quality, but large-volume audio files (WAV). There are several technologies that provide effective results against eavesdropping and modification of information sent during information exchange over the network**:** IPSec (Internet protocol security) protocol; VPN (Virtual Private Network) virtual private network; IDS (Intrusion Detection System) unauthorized access detection system. IPSec (Internet protocol security) allows for secure information exchange over the network using security protocols and encryption algorithms. This special standard ensures that programs, data, and hardware are compatible with each other when computers on a network communicate with each other.

Core Security Technologies

While not directly supporting the network, there are related cybersecurity technologies that can help protect the infrastructure:

Endpoint Detection and Response (EDR) security solutions continuously monitor all user and endpoint activity to protect against threats and detect suspicious behavior. They also offer investigation and incident response capabilities that can eliminate the threat and isolate the affected system from the rest of the network. DDoS Protection: DDoS protection protects against denial-of-service attacks that aim to take down a corporate network and disrupt operations. For example, FortiDDoS rapidly inspects data packets and automatically blocks unauthorized traffic from entering the network.

Conclusion.

Network security is provided by modern technologies and methods, but the problems and threats in this area are constantly evolving. The results of the study showed that the most effective results can be achieved by integrating the technologies used to ensure network security, such as cryptographic methods, IDS/IPS systems, VPN, and security policies. At the same time, each of these technologies has its own weaknesses, which require constant updating and improvement. Cryptographic methods, such as AES and RSA algorithms, play an important role in data encryption, but in some cases their security has been tested by powerful attacks. Therefore, it is necessary to develop new and advanced encryption technologies. Also, IDS/IPS systems can detect more than 85% of dangerous activities in the network, but they may lose their effectiveness depending on the complexity of the network and the volume of data. This highlights the need to improve systems and apply new methods. Although VPN technologies are also effective in ensuring network security, the weaknesses of some VPN services can pose a threat to data security. Therefore, it is necessary to ensure a high level of encryption and strengthen user security when implementing VPN systems. Not only technologies, but also user behavior play an important role in ensuring network security. Many security problems are caused by users choosing the wrong passwords or mismanaging access rights to the system. In order to develop effective strategies for ensuring network security, it is necessary to constantly monitor

new threats emerging in the network and apply new methodologies. For example, sophisticated threats such as DDoS attacks can lead to network vulnerability, but advanced methods have been developed to detect and block these threats. Improving network monitoring and security systems is important in combating such attacks.

References

1. **Ahmedov, J. A., & Qurbonov, M. (2020).** *Fundamentals of Information Technologies.* Tashkent: Fan va Texnologiya.
2. **Anderson, R. (2020).** *Security Engineering: A Guide to Building Dependable Distributed Systems (3rd ed.).* Wiley.
3. **Berdiev, B. (2019).** *Computer Networks and Security Fundamentals.* Tashkent: Iqtisodiyot.
4. **Kurose, J. F., & Ross, K. W. (2021).** *Computer Networking: A Top-Down Approach (8th ed.).* Pearson.
5. **Law of the Republic of Uzbekistan.** (2022, April 15). *On Cybersecurity.* No. O‘RQ-764.
6. **National Institute of Standards and Technology (NIST).** (2020). *Special Publication 800-207: Zero Trust Architecture.* U.S. Department of Commerce.
7. **Stallings, W. (2022).** *Cryptography and Network Security: Principles and Practice (8th ed.).* Pearson.
8. **Tanenbaum, A. S., & Wetherall, D. J. (2019).** *Computer Networks (6th ed.).* Prentice Hall.
9. **IEEE Xplore Digital Library. (2024).** *Current Trends in Network Security and AI-driven Monitoring.* [Online resource].
10. **Zimmermann, P. R. (2021).** *Post-Quantum Cryptography and the Future of Data Encryption.* Journal of Cybersecurity and Hardware Defense.