EAI Endorsed Transactions
on Internet of Things
Research Article EAI.EU

Security Methods to Improve Quality of Service

Nidhi Agarwal[1,*], Anjali[1], Anuj Singh Chauhan[1], Ankit Kumar[1]

[1] Department of Computer Science Engineering, Galgotias University, Greater Noida, UP, India

Abstract

INTRODUCTION: Security and Quality of Service (QoS) are two of the most critical aspects of communication networks. Security measures are implemented to protect the network from unauthorized access and malicious attacks, whereas QoS measures are implemented to ensure that the network is reliable, efficient, and can meet the demands of users.
OBJECTIVES: This paper examines various methods of network security and their impact on the quality of service (QoS) in computer networks. The study analyses different types of network attacks, such as denial of service (DoS), distributed denial of service (DDoS), and intrusion attempts, and their impact on QoS. The paper also explores various security mechanisms, such as intrusion detection and prevention systems (IDPS), firewalls, virtual private networks (VPNs), and techniques for encryption, that can help mitigate network security threats while maintaining QoS.METHODS: The study evaluates the strengths and weaknesses of the security mechanisms in terms of their ability to provide protection against network attacks while minimizing the impact on QoS.
RESULTS: The paper provides recommendations for organizations to enhance their network security posture while improving the QoS, such as implementing robust network security policies, investing in advanced security tools, and training employees to recognize and respond to network security incidents.
CONCLUSION: This paper offers a comprehensive analysis of network security methods and their impact on QoS, providing insights and recommendations for organizations to improve their network security posture and maintain a high level of QoS.hese are the conclusions of this paper.

Keywords: network security, dos, ddos, idps, vpns, encryption

Received on 02 October 2023, accepted on 05 December 2023, published on 13 December 2023

doi: 10.4108/eetiot.4587

1. Introduction

Security and Quality of Service (QoS) are two of the most critical aspects of communication networks. Security measures are implemented to protect the network from unauthorized access and malicious attacks, whereas QoS measures are implemented to ensure that the network is reliable, efficient, and can meet the demands of users. However, the implementation of security measures often leads to reduced QoS [1-3], leading to slower network performance, increased latency, and other issues. Therefore, it is essential to find a balance between security and QoS to provide a seamless and secure network experience to users. In recent years, several security methods have been developed and implemented to improve network security while maintaining optimal QoS.

This review paper aims to examine the effectiveness of different security methods in enhancing the QoS of communication networks. Specifically, we will discuss [4,5] various security methods such as encryption, intrusion detection systems, firewalls and network access control, among others, and their impact on the QoS of communication networks. Overall, this review paper aims to provide a comprehensive understanding of the different security methods that can be used to enhance the QoS of communication networks. By examining the various methods [6-8] and their impact on network performance, this review paper will provide insights into how security

*Corresponding author. Email: nidhiagarwal82@gmail.com

attacks, such as phishing and spear-phishing, can trick users into divulging sensitive information or clicking on malicious links.

In summary, the open and decentralized nature of the internet architecture makes it vulnerable to various security risks. Addressing these vulnerabilities requires a multi-layered approach that includes implementing security protocols, educating users, and regularly updating and patching systems.

2.3. Common internet attack method

There are numerous internet attack methods used by attackers to exploit vulnerabilities in computer systems and networks. Some of the most common internet attack methods include:

Malware: Malware, also known as malicious software, refers to software specifically created to inflict damage upon computer systems or networks. This category encompasses viruses, Trojans, and spyware, which can be transmitted through email attachments, downloads from untrustworthy websites, or infected removable media.

Phishing: Phishing constitutes a form of social engineering attack aimed at deceiving users into revealing confidential information, including usernames, passwords, and credit card details. These fraudulent activities are commonly executed via email, instant messaging, or social media platforms.

Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks: These attacks entail inundating a website or network with an excessive amount of traffic, rendering it inaccessible to genuine users. Denial of Service (DoS) attacks originate from a single source, whereas Distributed Denial of Service (DDoS) attacks harness multiple sources to generate a higher volume of traffic.

Man-in-the-middle (MitM) attacks: Man-in-the-Middle (MitM) attacks occur when an unauthorized entity intercepts and monitors or alters the content of communications between two parties. Typically, these attacks target unsecured wireless networks.

SQL injection: SQL injection is an attack method that specifically focuses on web applications, wherein malicious SQL statements are injected into the application's database. The purpose is to illicitly acquire sensitive information or manipulate the contents of the database.

Cross-site scripting (XSS): Cross-Site Scripting (XSS) attacks consist of inserting malicious code into a website with the intention of pilfering user data, such as cookies or session tokens. Typically, this attack method is executed via susceptible web forms or search fields. [20-22]

Ransomware: Ransomware refers to a form of malicious software that encrypts files belonging to a target individual or organization, demanding a ransom payment in return for the decryption key. Commonly, ransomware is distributed through phishing emails or malicious downloads.

2.4. Security issues of IP protocol IPv6 and IPv4

Both IPv4 and IPv6 are Internet Protocols these are utilized for the purpose of recognizing and establishing communication with devices within a network. However, there are several security issues associated with IPv6 that are not present in IPv4. Some of the security issues of IPv6 include:

Address space: IPv6 provides a much larger address space than IPv4, which means that it can support a large number of devices on a network. However, this also makes it more difficult to scan for and identify devices that may be vulnerable to attacks.

Fragmentation: IPv6 does not rely on fragmentation of packets like IPv4 does, which can create problems for devices that are not able to process large packets. This can lead to packet loss and delays in communication.
Neighbour discovery: While utilizing IPv6, the Neighbour Discovery Protocol (NDP) is utilized to detect and locate other devices within the network. However, it is important to note that malicious actors can exploit NDP for conducting attacks such as address spoofing and denial of service (DoS) attacks.

Autoconfiguration: Within IPv6, there is a functionality known as stateless address autoconfiguration (SLAAC), enabling devices to autonomously set up their IPv6 addresses without relying on a DHCP server.
However, this can also make it easier for attackers to obtain network addresses and carry out attacks.

IPsec: IPv6 includes support for IPsec, a protocol that is used to encrypt and authenticate network traffic. However, the implementation of IPsec in IPv6 is not standardized, which can create interoperability issues between different devices.

Overall, IPv6 introduces several new security issues that are not present in IPv4. It is important for network administrators and security professionals to be aware of these issues and take steps to secure their networks accordingly. This may include implementing firewalls, intrusion detection systems, and other security measures to protect against attacks.

2.5. Security in different networks

Security in different networks can vary depending on the specific characteristics of each network. Here are some examples of security considerations in different types of networks:

(i) Local Area Networks (LANs): LANs are typically used to connect devices within a small geographic area, such as a home or office. Security in LANs can be enhanced through the use of firewalls, access controls, and intrusion detection systems.
(ii) Wide Area Networks (WANs): WANs are used to connect devices across larger geographic areas, such as different offices or cities. WANs can be secured through the use of Virtual Private Networks (VPNs), which encrypt traffic between devices and provide secure remote access to the network.
(iii) Wireless Networks: Data transmission in wireless networks relies on the utilization of radio waves, rendering them vulnerable to interception and various other attacks. To bolster security within wireless networks, measures such as encryption, robust passwords, and the implementation of Wi-Fi Protected Access (WPA) protocols can be employed.
(iv) Cloud Networks: Cloud networks are used to store and access data and applications over the internet. Security in cloud networks can be enhanced through the use of strong authentication mechanisms, data encryption, and monitoring tools to detect and respond to potential security threats.
(v) Industrial Control Systems (ICS): ICS networks are used to control industrial processes such as manufacturing, transportation, and energy production. Security in ICS networks can be enhanced through the use of firewalls, access controls, and intrusion detection systems, as well as specialized security measures such as air-gapped networks and security-focused operating systems.

Overall, security considerations in different networks will depend on factors such as the size and complexity of the network, the type of data being transmitted, and the potential consequences of a security breach. It is important to carefully evaluate the specific security needs of each network and implement appropriate security measures to mitigate the risk of attacks.

3. Current methods used in network security

There are a variety of methods used in network security to protect against cyberattacks and safeguard sensitive data. Here are some of the most commonly used methods:

Firewalls: Firewalls serve as a fundamental security mechanism employed to selectively control both inbound and outbound network traffic, employing a predefined set of rules. They can be realized in the form of either hardware or software and are generally considered the initial layer of defence in a network security approach.

Intrusion Detection and Prevention Systems (IDPS): IDPS are used to detect and respond to potential security threats by analysing network traffic and identifying patterns that may indicate an attack. They can be used to alert network administrators to suspicious activity or take automated actions to prevent an attack.

Virtual Private Networks (VPNs): Virtual Private Networks (VPNs) are utilized to establish a secure link between distant devices via the internet. Encryption is employed to safeguard data transmitted through this connection, enabling secure remote access to a network.

Access Controls: Access controls are used to restrict access to network resources based on the identity of the user or device. They can be used to prevent unauthorized access to sensitive data and limit the potential damage caused by a security breach.

Encryption: The purpose of encryption is to safeguard data by transforming it into an illegible format that can only be deciphered using a specific decryption key. Encryption serves to protect both data transmitted over networks and data stored on devices.

Multi-factor Authentication (MFA): MFA is used to enhance the security of authentication mechanisms by requiring multiple forms of authentication to verify the identity of a user. This can include something the user knows (such as a password), something they have (such as a security token), or something they are (such as biometric data).

Security Information and Event Management (SIEM): SIEM is used to collect and analyse data from various sources within a network to identify potential security threats. It can be used to correlate data from multiple sources to provide a more complete picture of network activity and help detect and respond to security incidents.

Overall, a combination of these methods is typically used in network security to create a multi-layered defence that can protect against a variety of potential security threats.

4. Investigation of the role of employee training and awareness in enhancing network security

Employee training and awareness are critical components of a comprehensive network security strategy. Here are some potential areas of research related to this topic: Evaluating the effectiveness of different types of employee

training programs, such as classroom-based training, e-learning, and simulation exercises. Investigating the role of employee motivation and engagement in enhancing the effectiveness of security awareness training. Assessing the impact of different communication strategies, such as newsletters, email alerts, and posters, in reinforcing security awareness and promoting best practices. Studying the effectiveness of gamification techniques in enhancing employee engagement and motivation in security awareness training. Investigating the impact of security culture and organizational norms on employee behaviour and the effectiveness of security awareness training.

Overall, research in this area can help organizations to better understand the factors that influence employee behaviour and the effectiveness of security awareness training. By identifying best practices and developing more effective training programs, organizations can reduce the risk of data breaches and cyberattacks. Development of new network security technologies and methods that can effectively address emerging security threats. The development of new network security technologies and methods is crucial to effectively address emerging security threats. Here are some potential areas of research: Investigating the use of blockchain technology in enhancing network security, such as the use of decentralized authentication systems and distributed ledger technology for securing network transactions. Developing new intrusion detection and prevention techniques that leverage advanced machine learning and artificial intelligence algorithms to detect and respond to emerging threats. Studying the effectiveness of new cryptographic techniques, such as post-quantum cryptography, in protecting network communications from quantum computing-based attacks.

Investigating the use of software-defined networking (SDN) and network functions virtualization (NFV) to enhance network security by enabling more granular control over network traffic and facilitating the deployment of security policies. Developing new methods for detecting and preventing insider threats, such as the use of behaviour-based analytics and user activity monitoring. Overall, research in this area can help to develop new network security technologies and methods that are better suited to address emerging security threats. By staying ahead of the evolving threat landscape, organizations can better protect their networks and data from cyber-attacks. Studying the impact of network topology on the effectiveness of network security measures, including the use of segmentation and micro segmentation to isolate critical assets and limit the spread of cyberattacks.

The impact of network topology on the effectiveness of network security measures is an important area of research, as it can help organizations to better understand how to protect their critical assets from cyber-attacks. Here are some potential areas of research: Investigating the impact of network segmentation on the effectiveness of network security measures, including the use of virtual LANs (VLANs) and firewalls to isolate critical assets from the rest of the network. Studying the effectiveness of micro segmentation techniques, which involve breaking down the network into smaller segments and applying more granular security policies to each segment.

Assessing the impact of network topology on the deployment and effectiveness of intrusion detection and prevention systems (IDPS), including the use of distributed IDPS sensors to cover different parts of the network. Investigating the effectiveness of different network topologies, such as hub-and-spoke vs. mesh networks, in limiting the spread of cyber-attacks and reducing the impact of a successful breach. Studying the impact of software-defined networking (SDN) and network functions virtualization (NFV) on network topology and its effect on network security measures.

Overall, research in this area can help organizations to better understand the impact of network topology on the effectiveness of network security measures, and to develop more effective security strategies that take into account the unique characteristics of their network topology. By implementing appropriate segmentation and micro segmentation techniques, organizations can limit the potential impact of cyber-attacks and better protect their critical assets.

5. Conclusion

In conclusion, investigating the effectiveness of network security measures in protecting against emerging threats is a critical area of research that is essential for organizations to stay ahead of the ever-evolving cybersecurity landscape. As new threats such as fileless malware and zero-day exploits emerge, organizations must develop new strategies to protect their critical assets and data. Evaluating the effectiveness of different types of anti-malware software, sandboxing techniques, network segmentation and microsegmentation, behavioral-based detection and response techniques, and emerging technologies such as the Internet of Things and cloud computing, are all important research areas that can provide valuable insights into how organizations can better protect themselves against these threats.

By staying informed about the latest research in network security and investing in the development of new technologies and techniques, organizations can stay ahead of the curve and mitigate the risks associated with emerging threats. It is crucial for organizations to continuously review and update their security policies and strategies to ensure they are properly prepared to defend against the constantly evolving cybersecurity landscape.

5. Future work

Further research on the effectiveness of other network security measures, such as firewalls and intrusion detection systems. Investigation of the role of employee training and awareness in enhancing network security. Development of new network security technologies and methods that can effectively address emerging security threats. Exploration of the ethical and legal implications of network security measures, including issues related to privacy and data protection.

Integration of network security measures with broader cybersecurity strategies, such as incident response planning and risk management. Further research on the effectiveness of other network security measures, such as firewalls and intrusion detection systems: Further research on the effectiveness of other network security measures such as firewalls and intrusion detection systems can help to improve the overall security of computer networks. Here are some potential areas of research. Evaluating the effectiveness of next-generation firewalls (NGFWs) that incorporate advanced threat detection and prevention capabilities, such as deep packet inspection and behavioural analysis. Investigating the use of machine learning and artificial intelligence in intrusion detection and prevention systems (IDPS) [2] to enhance their ability to detect and respond to sophisticated cyberattacks.

Comparing the effectiveness of different types of firewalls and IDPSs, such as hardware vs. software-based solutions, open-source vs. commercial solutions, and cloud-based vs. on-premises solutions. Studying the impact of network topology on the effectiveness of network security measures, including the use of segmentation and micro segmentation to isolate critical assets and limit the spread of cyberattacks. Investigating the effectiveness of network security measures in protecting against emerging threats, such as fileless malware and zero-day exploits. Overall, further research on the effectiveness of different network security measures can help organizations to make informed decisions about the best security strategies to [3,7-9] implement in order to protect their networks from cyber threats.

References

[1] Anna D Gage; Hannah H Leslie; Asaf Bitton; J Gregory Jerome; Jean Paul Joseph; Roody Thermidor; Margaret E Kruk; "Does Quality Influence Utilization of Primary Health Care? Evidence From Haiti", GLOBALIZATION AND HEALTH, 2018.

[2] Bereket Yakob; Anna Gage; Tsinuel Girma Nigatu; Sarah Hurlburt; Seifu Hagos; Girmaye Dinsa; Diana Bowser; Peter Berman; Margaret E Kruk; Ephrem Tekle; "Low Effective Coverage Of Family Planning And Antenatal Care Services In Ethiopia", INTERNATIONAL JOURNAL FOR QUALITY IN HEALTH CARE : 2018.

[3] Dwi Suhartanto; Mohd Helmi Ali; Kim Hua Tan; Fauziyah Sjahroeddin; Lusianus Kusdibyo; "Loyalty Toward Online Food Delivery Service: The Role of E-service Quality and Food Quality", JOURNAL OF FOODSERVICE BUSINESS RESEARCH, 2019.

[4] Youngjoon Choi; Miju Choi; Munhyang (Moon) Oh; Seongseop (Sam) Kim; "Service Robots in Hotels: Understanding The Service Quality Perceptions of Human-robot Interaction", JOURNAL OF HOSPITALITY MARKETING & MANAGEMENT, 2019.

[5] Francis Palma; Naouel Moha; Yann-Gaël Guéhéneuc; "UniDoSA: The Unified Specification and Detection of Service Antipatterns", IEEE TRANSACTIONS ON SOFTWARE ENGINEERING, 2019.

[6] Yan Li; Huping Shang; "Service Quality, Perceived Value, and Citizens' Continuous-use Intention Regarding E-government: Empirical Evidence from China", INF. MANAG., 2020.

[7] Takeshi Morita; Naho Kashiwagi; Ayanori Yorozu; Hideo Suzuki; Takahira Yamaguchi; "Evaluation of A Multi-robot Cafe Based on Service Quality Dimensions", THE REVIEW OF SOCIONETWORK STRATEGIES, 2020.

[8] Gerald G Singh; Ian M S Eddy; Benjamin S Halpern; Rabin Neslo; Terre Satterfield; Kai M A Chan; "Mapping Cumulative Impacts To Coastal Ecosystem Services In British Columbia", PLOS ONE, 2020.

[9] Yiwen Zhang; Guangming Cui; Shuiguang Deng; Feifei Chen; Yan Wang; Qiang He; "Efficient Query of Quality Correlation for Service Composition", IEEE TRANSACTIONS ON SERVICES COMPUTING, 2021.

[10] Sulemana Bankuoru Egala; Dorcas Boateng; Samuel Aboagye Mensah; "To Leave or Retain? An Interplay Between Quality Digital Banking Services and Customer Satisfaction", INTERNATIONAL JOURNAL OF BANK MARKETING, 2021. (IF: 3)

[11] Agarwal N., Jain A., Gupta A., Tayal D.K. (2022) Applying XGBoost Machine Learning Model to Succor Astronomers Detect Exoplanets in Distant Galaxies. In: Dev A., Agrawal S.S., Sharma A. (eds) Artificial Intelligence and Speech Technology. AIST 2021. Communications in Computer and Information Science, vol 1546. Springer, Cham. https://doi.org/10.1007/978-3-030-95711-7_33.

[12] Agarwal, N., Srivastava, R., Srivastava, P., Sandhu, J., Singh, Pratap P. Multiclass Classification of Different Glass Types using Random Forest Classifier. 6th International Conference on Intelligent Computing and Control Systems (ICICCS), 2022. p. 1682-1689.

[13] Agarwal, N., Singh, V., Singh, P. Semi-Supervised Learning with GANs for Melanoma Detection. 6th International Conference on Intelligent Computing and Control Systems (ICICCS), 2022. p. 141-147.

[14] Tayal, D.K., Agarwal, N., Jha, A., Deepakshi, Abrol, V. To Predict the Fire Outbreak in Australia using Historical Database. 10th International Conference on Reliability,

Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), 2022. p. 1-7.

[15] Agarwal, N., Tayal, D.K. FFT based ensembled model to predict ranks of higher educational institutions. Multimed Tools Appl 81, 2022.

[16] Wenjuan Li; Jian Cao; Keyong Hu; Jie Xu; Rajkumar Buyya; "A Trust-Based Agent Learning Model for Service Composition in Mobile Cloud Computing Environments", IEEE ACCESS, 2019.

[17] Tamara Radivilova; Lyudmyla Kirichenko; Dmytro Ageiev; Vitalii Bulakh; "The Methods To Improve Quality Of Service By Accounting Secure Parameters", ARXIV-CS.NI, 2019.

[18] Tian Wang; Pan Wang; Shaobin Cai; Ying Ma; Anfeng Liu; Mande Xie; "A Unified Trustworthy Environment Establishment Based on Edge Computing in Industrial IoT", IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, 2020.

[19] Rongbin Xu; Yongliang Cheng; Zhiqiang Liu; Ying Xie; Yun Yang; "Improved Long Short-Term Memory Based Anomaly Detection with Concept Drift Adaptive Method for Supporting IoT Services", FUTURE GENER. COMPUT. SYST., 2020.

[20] Zahir Tari; Adil Fahad; Abdulmohsen Almalawi; Xun Yi; "A Hybrid Clustering-classification for Accurate and Efficient Network Classification", 2020.

[21] Khalid F. Mahmmod; Mohammed M. Azeez; Mohamad A. Ahmed; "IPsec Cryptography for Data Packets Security Within VPN Tunneling Networks Communications", 2020 INTERNATIONAL CONFERENCE ON ELECTRICAL ENGINEERING AND ..., 2020.

[22] Dong-Won Kim; Jin-Young Choi; Keun-Hee Han; "Risk Management-based Security Evaluation Model For Telemedicine Systems", BMC MEDICAL INFORMATICS AND DECISION MAKING, 2020.

[23] Ghosh, H., Tusher, M.A., Rahat, I.S., Khasim, S., Mohanty, S.N. (2023). Water Quality Assessment Through Predictive Machine Learning. In: Intelligent Computing and Networking. IC-ICN 2023. Lecture Notes in Networks and Systems, vol 699. Springer, Singapore. https://doi.org/10.1007/978-981-99-3177-4_6

[24] Alenezi, F.; Armghan, A.; Mohanty, S.N.; Jhaveri, R.H.; Tiwari, P. Block-Greedy and CNN Based Underwater Image Dehazing for Novel Depth Estimation and Optimal Ambient Light. Water 2021, 13, 3470. https://doi.org/10.3390/w13233470

[25] G. P. Rout and S. N. Mohanty, "A Hybrid Approach for Network Intrusion Detection," 2015 Fifth International Conference on Communication Systems and Network Technologies, Gwalior, India, 2015, pp. 614-617, doi: 10.1109/CSNT.2015.76.