A Survey on Cybersecurity Measures and Network Safeguarding Techniques

Abivijay.S[1], Rithika Anand.P.K[2], Santhana Mahalingam.J[3], Rinisha.R[4]
[1]*Assistant Professor, Department of Computer Science, Shri Nehru Maha Vidyalaya College of Arts and Science, Coimbatore*
[2,3,4] *II M.Sc Computer Science, Shri Nehru Maha Vidyalaya College of Arts and Science, Coimbatore.*

Abstract: *Computers are vital in daily life, storing important data digitally. Encryption helps mitigate security risks. Managing network security involves a comprehensive strategy, cryptography and integrating network security. Research improves infrastructure and specialized systems maintain data integrity. Rapid technological advancement poses challenges, addressed in this paper.*

Keyword: *Computer network information; Information security; Security protection.*

I. INTRODUCTION

`The storage of vast amounts of data presents significant challenges for computer technology. Urgent solutions are required for various information security issues and tools. Traditional IT infrastructure falls short in meeting the demands of massive data storage. In the era of big data, prevalent and critical concerns in computer information security include data breaches, manipulation, Safeguarding information and unauthorized privacy data breaches. computer necessitates protection measures, network systematic coupled with proactive user engagement. Effective computer information security entails the coordinated deployment of diverse strategies to mitigate security risks and ensure data integrity. Only through this comprehensive approach can the likelihood of security breaches be minimized, providing assurance of data security.

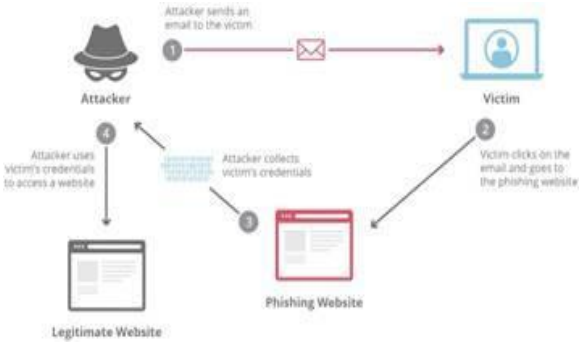
II. COMPUTER NETWORK INFORMATION SECURITY

2.1 Issue of Virus Attacks

Many users lack a strong understanding of safe practices while navigating computer networks. For instance, they may easily guess or crack others' account passwords, leading to theft of important accounts set up in a simplistic manner. Furthermore, malicious behaviors of other computer users contribute to information security breaches in computer networks. Such attacks encompass not only substantive network assaults aimed at compromising the integrity and security of networked information but also users' inadvertent susceptibility to attacks. Active attacks, exemplified by the prevalence of viruses in many computer networks in our country, pose significant threats. These viruses exhibit potent latent and infectious characteristics. Upon users clicking on links or editing programs infected with viruses, these viruses proliferate rapidly. They infiltrate executable programs, resulting in diminished system efficiency, duplication of pertinent information, or deletion of crucial files, thereby inflicting losses on computer network users [1]. The following example involving Alipay succinctly illustrates the impact of virus attacks on computer network information security. Alipay, a popular online payment platform, serves as a common means for cash transactions. Most users' mobile devices are equipped with Alipay software, which requires registration using personal information such as name, identity card number, code, collection numbers, and payment passwords, seemingly ensuring robust network security. However, as modern network attack techniques advance, criminals exploit vulnerabilities in Alipay's password function to access users' sensitive information. By vulnerabilities, exploiting perpetrators can these gain unauthorized access to Alipay accounts and conduct illicit money transfers.[6], [9]

2.2 Issue of Email Attacks

Email, renowned for its ease of dissemination and accessibility, poses a significant vulnerability in digital networks. Malicious actors exploit these traits by clandestinely sending emails containing viruses from compromised accounts, jeopardizing recipients' data security. Unauthorized use of email accounts to distribute malware exacerbates the threat. Addressing email attacks requires robust cybersecurity measures, user education, and proactive detection and neutralization of malicious content [2]. Organizations must continuously update their email security protocols and invest in advanced threat detection systems to stay ahead of evolving cyber threats. Additionally, fostering a culture of cybersecurity awareness among users is essential in mitigating the risks posed by email-based attacks.[8], [10]



2.3 Issue of Open Computer Networks and Unrestricted Application Downloads

Computer networks operate with an inherent openness, rendering them susceptible to exploitation to some extent. This openness facilitates the dissemination, transmission, and sharing of information with few restrictions, thereby creating opportunities for illicit activities. To promote the widespread adoption of computer network technology, the modern network application market offers a plethora of lifestyle apps and gaming software. These necessitate applications downloading for often user experience. In their quest for novelty, many users indiscriminately download various apps, including those of questionable origin or content such as security risks, unknown applications, or adult content websites.This indiscriminate downloading jeopardizes the security of their mobile devices or computer network systems. While most computer network systems incorporate tools and software to enhance service quality and system management, malicious actors can exploit these tools to gather illicit information and launch attacks on user data. [7], [9]

2.4 Issue of Hacker Intrusion

This deliberate destruction and manipulation of data by hackers have the potential to cripple computer network systems, resulting in substantial losses and disruptions to individuals' productivity, work, and daily life. Combatting hacker intrusion demands constant vigilance, proactive security measures, and ongoing updates to defense systems. Additionally, fostering a culture of cybersecurity awareness among users is paramount in thwarting hacker attacks and safeguarding network integrity.[6], [10], [12]

III. COMPUTER NETWORK INFORMATION SECURITY PROTECTION STRATEGY

3.1 Enhancement of Account Management

In computer networks, various types of accounts exist, and security issues often arise when illegal entities attempt to steal user account information and passwords. To mitigate such risks, network users are advised to enhance the complexity of their account passwords by incorporating combinations of numbers, letters, and symbols, rather than opting for simplistic passwords that are easily guessed or stolen. It is also recommended to refrain from using the same password for multiple accounts, as this increases the likelihood of password theft.

3.2 Enhancement of Effective Utilization of Firewall Technology

In the realm of computer network security, firewall technology stands as a pivotal tool to safeguard information integrity. Therefore, in the era of big data, it is imperative to bolster the effective utilization of firewall systems or security mechanisms to ensure the smooth operation of computer networks. For instance, within enterprise computer applications, the volume and significance of involved information necessitate the establishment of comprehensive data security measures to foster a culture of heightened awareness among management personnel regarding computer network security. Particularly in the context of the big data era, strengthening the utilization of firewall technology is essential to mitigate the adverse effects of virus and hacker intrusions on network security. Firewall technology plays a crucial role in thwarting malignant software by effectively isolating viruses, while the implementation of topological structures enhances the security and reliability of computer network operations. Moreover, prioritizing the use of firewall technology for regular data maintenance and repairs significantly curbs virus invasions. As computer technology continues to advance, the evolving nature and diversity of viruses demand that Internet technical managers possess comprehensive understanding and proficiency in identifying and combating virus characteristics, thus enabling them to implement effective preventive measures tailored to the evolving threat landscape.[2], [10]

3.3 Enhancement of Antivirus Software and Email Recognition System Utilization

As computer network information security incidents become increasingly prevalent, the utilization of antivirus software in computer operations has surged, playing a pivotal role in fortifying the security of computer network operations and thwarting threats such as viruses and spam messages. Therefore, in the era of big data, it is imperative to reinforce the effective application of antivirus software and email recognition systems. Antivirus software can be seamlessly integrated with firewall technology to identify viruses and malignant software intercepted by the firewall, subsequently executing effective antivirus measures to detect and eliminate latent viruses within the computer system. Meanwhile, email recognition systems serve as crucial security mechanisms for combating spam. Given that many viruses and malicious software infiltrate computers through email, email recognition systems play a vital role in identifying and filtering potentially harmful emails

3.4 Implementation of Digital Signatures and File Encryption

Commercial encryption software primarily operates through encryption algorithms, with examples including widely-used folder encryption software like the Master of Encryption. Following file encryption, only authorized users can access the encrypted files via their account login credentials, as reinstalling the system would render the encrypted files inaccessible without the established account credentials. To mitigate potential complications, it is advisable to exercise caution when utilizing file encryption functions, preferably restricting their use to files of a confidential or highly sensitive nature. Moreover, when encrypting files, it is prudent to create backups and store them in alternative locations to prevent data loss or accessibility issues.[3], [11]

IV. CONCLUSION

Investigating methods to enhance computer network security is paramount in safeguarding the information security and interests of network users. Given the prevalence of threats such as virus attacks, email intrusions, unrestricted network access, indiscriminate application downloads, and hacker breaches, it is imperative to bolster network security measures.

Strengthening account management, protective barriers, antivirus solutions, email filtering systems, and implementing digital signature and file encryption technologies are essential steps in fortifying network information security. These proactive measures are vital in mitigating risks and ensuring the integrity and confidentiality of networked data.[1], [5], [12]

REFERENCES

[1] B. B. Gupta, G. Martinez Perez, D. P. Agrawal, and D. Gupta, *Handbook of Computer Networks and Cyber Security: Principles and Paradigms*, Springer, 2015.

[2] W. Stallings, *Network Security Essentials: Applications and Standards*, 6th ed., Pearson Education, 2017.

[3] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd ed., John Wiley & Sons, 1996.

[4] C. Sanders, *Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems*, 2nd ed., No Starch Press, 2011.

[5] R. J. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd ed., Wiley, 2008.

[6] J. Erickson, *Hacking: The Art of Exploitation*, 2nd ed., No Starch Press, 2008.

[7] A. S. Tanenbaum and D. J. Wetherall, *Computer Networks*, 5th ed., Pearson Education, 2011.

[8] C. Pfleeger and S. L. Pfleeger, *Security in Computing*, 5th ed., Prentice Hall, 2015.

[9] D. Gollmann, *Computer Security*, 3rd ed., Wiley, 2011.

[10] K. Scarfone and P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)," NIST Special Publication 800-94, National Institute of Standards and Technology, 2007.