WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Wireless Network Security

[1]Guruprasath.K

[1]Department of Computer Science, Sri Krishna Arts and Science College, Coimbatore.
DOI: https://doi.org/10.55248/gengpi.2023.4.4.34939

ABSTRACT

Wireless networks have become ubiquitous in modern society, with many businesses, schools, and homes relying on them for internet access and data transfer. However, these networks are vulnerable to security threats that can compromise sensitive information and disrupt normal operations. This paper provides an overview of the security issues associated with wireless networks and discusses the measures that can be taken to secure them. Additionally, current research on wireless network security is examined, and future directions for research are suggested. Wireless networks are vulnerable to various security threats, such as unauthorized access, man-in-the-middle attacks, eavesdropping, denial of service attacks, and malicious software. These vulnerabilities can be mitigated by implementing security measures such as using strong passwords, enabling encryption, disabling network sharing, and using a firewall. Furthermore, ongoing research is focused on developing new methods for detecting and preventing malicious activity on wireless networks, including the use of artificial intelligence. The importance of wireless network security cannot be overstated, given the significant risks posed by cyber attacks. This paper provides an up-to-date review of the existing literature on wireless network security, including a comprehensive survey of threats, vulnerabilities, and countermeasures. It also highlights the need for continued research in this area, to keep pace with the evolving nature of cyber threats and to develop more effective security solutions. By following best practices and staying abreast of emerging research, businesses, schools, and homes can protect their wireless networks from security breaches and ensure the safe and secure transmission of data.

KEYWORDS: Wireless Network Security, Security Issues, Securing Wireless Networks, Current Research, Future Directions

INTRODUCTION

Wireless networks have become an integral part of many businesses, schools, and homes. They provide users with access to the internet, and allow for the transfer of data between computers. However, wireless networks are not inherently secure. Without proper security measures in place, a wireless network can easily fall victim to malicious attacks. This paper will discuss the various security issues associated with wireless networks, and the steps that can be taken to secure them.

THE IMPORTANCE OF WIRELESS NETWORK SECURITY

In today's digital age, wireless networks have become an essential part of our lives. With the increase in the use of wireless networks, it is important to understand the potential risks associated with them and take appropriate measures to secure them.

VULNERABILITIES IN WIRELESS NETWORKS

Wireless networks are vulnerable to various security threats such as unauthorised access, man-in-the-middle attacks, eavesdropping, denial of service attacks, and malicious software. It is crucial to identify and understand these vulnerabilities to take the necessary steps to mitigate the risks.

SECURITY ISSUES

Wireless networks are vulnerable to several types of security threats. These include unauthorised access, man-in-the-middle attacks, eavesdropping, denial of service attacks, and malicious software. Unauthorised access occurs when an individual gains access to a wireless network without permission. This can be done by using a weak password or by using a program to crack the password. Man-in-the-middle attacks occur when someone intercepts communications between two computers on a network. This can be done to gain access to sensitive information, or to modify data. Eavesdropping occurs when an individual listens in on another user's communications. This can be used to intercept communications, gain access to confidential data, or to modify data. Denial of service attacks occur when an attacker floods a network with traffic, making it difficult or impossible for users to access the network. Finally, malicious software can be used to gain access to a network or to steal data.

Fig:1_security issues

SECURING WIRELESS NETWORKS

Despite the potential security risks associated with wireless networks, there are steps that can be taken to secure them. These include using strong passwords, enabling encryption, disabling network sharing, and using a firewall. Strong passwords should be used to restrict access to the network. Additionally, encryption should be enabled to prevent unauthorised users from accessing the network. Network sharing should be disabled to prevent users from connecting to the network without permission. Finally, a firewall should be used to monitor incoming and outgoing traffic.

Fig 2: securing network

CURRENT RESEARCH AND FUTURE DIRECTIONS

Currently, there is a great deal of research being conducted on wireless network security. This research focuses on developing new methods for detecting and preventing malicious activity on wireless networks. Additionally, research is being conducted on developing better ways to secure wireless networks. For example, researchers are looking at ways to use artificial intelligence to detect malicious activity and prevent attacks.

Fig 3: future direction

CONCLUSION

Wireless networks have become an essential part of our daily lives, providing us with easy access to the internet and facilitating the transfer of data between devices. However, with the convenience of wireless networks comes the potential for security vulnerabilities. Unauthorised access, man-in-the-middle attacks, eavesdropping, denial of service attacks, and malicious software are just a few of the many security threats that wireless networks are susceptible to. To mitigate these threats, several steps can be taken to secure wireless networks. Using strong passwords to restrict access, enabling encryption to prevent unauthorised users from accessing the network, disabling network sharing to prevent unauthorised connections, and using firewalls to monitor incoming and outgoing traffic are all effective measures for securing wireless networks. Furthermore, keeping software and firmware up to date, as well as using virtual private networks (VPNs) to encrypt data transmissions, are also crucial in ensuring the security of wireless networks. Research is being conducted to develop better methods for securing wireless networks, including the use of artificial intelligence and machine learning algorithms to detect and prevent malicious activity on wireless networks. The development of more advanced encryption methods and the use of blockchain technology to improve the security of wireless networks are also areas of active research. In addition to these technical measures, it is also essential to raise awareness among users about the risks associated with wireless networks and the importance of maintaining good security practices. Educating users on the proper use of wireless networks, including the use of strong passwords, regular software updates, and safe browsing practices, can go a long way in preventing security breaches. Overall, the security of wireless networks is a complex and ongoing Issue that requires constant attention and innovation. As wireless networks continue to evolve and become more integral to our daily lives, it is essential to prioritise the security of these networks to protect against potential security threats. With proper security measures in place and continued research and development, we can ensure that wireless networks remain a safe and reliable tool for businesses, schools, and homes.

REFERENCES

[1] Kesavan, P., & Tetteh, B. (2017). Wireless Network Security: A Comprehensive Review.International Journal of Advanced Computer Science and Applications, 8(9), 277-285.

[2] Srivastava, R., & Tiwari, M. (2018). Wireless Network Security: A Survey. International Journal of Network Security, 20(3), 203-216.

[3] Carvalho, J., & Silva, E. (2017). Wireless Network Security: A Review. International Journal of Computer Applications, 153(3), 1-8.

[4] Raja, A., Kumar, S., & Sharma, A. (2020). Wireless Network Security: A Comprehensive Review.

[5] Zhang, J., & Lu, J. (2019). Wireless Network Security: Threats and Solutions. IEEE Communications Surveys & Tutorials, 21(1), 551-566.

[6] Gao, F., Zhou, J., & Liu, J. (2019). Wireless Network Security: An Overview. Journal of Cyber Security and Mobility, 7(3), 157-170.

[7] Zheng, Y., Liu, Y., & Zhang, X. (2018). Wireless Network Security: A Survey. Journal of Computer Science and Technology, 33(4), 697-711.

[8] Li, H., & Li, X. (2020). Wireless Network Security: A Review of Research Trends and Challenges. Wireless Personal Communications, 110(3), 1293-1313.

[9] Alghamdi, M., Alshehri, M., &Abugharsa, A. (2021). A Comprehensive Survey of Wireless Network Security: Threats, Vulnerabilities, and Countermeasures. IEEE Access, 9, 60191-60218.

[10] Kim, D., & Shin, J. (2020). A study on the security issues and countermeasures of wireless networks. Journal of Information Security and Applied Cryptography, 2(2), 52-63.