Wireless Network Security

Adil Ergazin, Nurkhan Zaulanbay

***Abstract*—In our exploration, we covered the brief common information about wireless network security. In the beginning, the clarified issue navigated to briefly touch on the theme of wireless network security, kinds of varieties, and tips for being protected from gaining access and other hacker actions. Although, the research theme, the cordless network that spreads to endpoints wirelessly without cables consists of things such as the sharing method called share points from one access point, Wi-Fi, and their built architecture and security. And they were included in the research on wireless network security. Further, in getting more specified in wireless networks and their security, the stages of wireless network workflow were instantiated in step-by-step insights. Generally, after the process of brief insights we've split into two necessary to society's digital world the instructions and unique guarded wireless network architectures or models, exactly to individuals and enterprises about using wireless networks to be protected from anyone gaining access and other hackers actions. In the methodology part, additionally, the tips against hackers were provided to be safe. As such a bit known models of wireless network security are concretized in the methods section. In the observation about wireless connections, the physical actions against issues with hackers from being hacked by radiowaves were included and wrapped by examining its work processes of covering zone-bound restrictions. However, the outcomes were satisfactory, although we must comprehend the aspects of working wireless networks and how to be protected from attackers and data leaks. Furthermore, to obtain these insights, we might see them in methods sections and additionally by observing whole parts of the research.**

***Index Terms*—WPA, WPA2, WPA2, WPA3, WEP, network security, wireless network security, wireless network, IEEE 802.11, Wi-Fi, WPA2-Personal**

I. Introduction

Wireless network security is defined as the connection without any cables and by radio waves but with security stuff including encryption and protected protocols, tunnels, and cryptographic schemes against hacking, unauthorized access, and malicious actions. The research focused on a brief touch on the theme of wireless network security, kinds of varieties, tips for being protected from gaining access, and other hacker actions. Generally, wireless networks fork into several types of gathering access, such as Wi-Fi to the internet access, Bluetooth, and share access points. However, in the current research, we examined especially Wi-Fi and share access points that might require any such kind of physical device as called network devices and end devices. Basically, according to Kavianpour and Anderson in 2017, Wi-Fi is founded on IEEE 802.11 and uses encrypted protocols for connecting devices. By considering this argument and relying on the research of Adame, Carrascosa-Zamacois, and Bellalta in March of 2020, we might concrete that 802.11 splits into fame sections by adding its letters as m, n, l, and continuing. They are staged up to the current year with the new version 802.11be which was accepted in 2020 and supports radio wave connections to create computer networks. In the process of possessing entrance through a shared access point, network traffic moves through the encryption system protocols and, additionally, might conduct the connection among VPN configurations to each device by default. Further, the wireless network security objective consists of four stages of step-by-step connecting. These stages provide interaction with end devices, starting with access methods such as open, shared, and EAP (Extensible Authentication Protocol) authentications. If we move to the next level, it consists of insights into cryptography-protecting systems and the ways of guarding against malicious entrances, as called cryptographic protocols. The third part that is required for wireless networks is called authentication protocols. On account of the connection possessed among network-needed devices and net devices that demand special devices and instructions to interact with them, we contained it in the wireless access architecture part at the physical level.

A. *Wireless Network Security Stages*

*1) **Wireless access principles:*** Belonging to the wireless access methods step, as mentioned in the introduction paragraph, it encloses three main wireless varieties of connection, as way as PSK (Shared authentication uses a pre-shared key), open internet, and EAP (Extensible Authentication Protocol). As is well known about the open internet, and particularly this class of authentication, it does not possess to encrypted one acquiring less protection. In open authentication, security is not reliable and might not mandate any attempt to guess passwords, exactly obtaining no password requirements meaning its connection manner. In the phase of pre-sharing keys, beginning from network devices (sharing access point, router) to end points must instruct the same key on the leading device and to the connection receiving point as a password. It is commonly used for personal networking and small-scaled communities. However, there would be necessary, furthermore, large-scale networking, for instance, for enterprises and companies that needed to be secure from being attacked. It is called the Extensible Authentication Protocol, where the overcontrol of companies under hacker management is harmful to them as a creepy nightmare, and on account of that, it handles the authentication of the Wi-Fi LAN of the organization among the servers to not ensure this kind of inner situation.

*2) **Wireless network security protocols:*** The security part formed of cryptographic protocols WPS (Wi-Fi Protected Setup) mounting the operation of network devices and end devices wayt lighter and additionally made with four major protocols, such as WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), WPA2 (Wi-Fi Protected Access Version 2), WPA3 (Wi-Fi Protected Access Version 3). Further, if close shift to the WPS feature, it should be minimized, exactly required to be turned off. In line with less security stuff included WEP, but useful for nowadays in old types of equipment. The way defended protocols used for us WPA2, WPA3.

*3) **Authentication security protocols**:* In the intricate realm of wireless network security, where the essence lies in the safeguarding of connections, we find ourselves focused on ensuring integrity. Meet the guards of this digital fortress—authentication security protocols standing tall, making sure that only those considered worthy can enter the network gates. Two strong defenders emerge, each with its unique abilities—the 802.1X/EAP protocol and the respected RADIUS system, champions of the cyber world.

Imagine the 802.1X/EAP protocol, a watchful figure wearing the armor of security, a partner of WPA and WPA2 in the big defense dance. With the simplicity of the Extensible Authentication Protocol (EAP), it coordinates a dance of secure key exchange and user authentication. This method, a virtuoso in its own right, not only strengthens the network's security but also ensures that only those armed with the keys of valid credentials can navigate its digital pathways.

Now, shift your focus to the other side, where RADIUS, an acronym carrying the weight of Remote Authentication Dial-In User Service, plays a crucial role in the big stages of enterprise environments. Picture a centralized conductor leading the authentication symphony on a dedicated server, strengthening the network's defenses with a harmonious mix of order and security. This centralized approach, a choreography of efficiency, not only simplifies the management of users but also extends its kindness to support various authentication methods—a flexible yet strong security structure, a masterpiece created on the canvas of enterprise resilience.

*4) **Wireless network security installation**:* In moving from the abstract world of authentication theory to the practicalities of implementation, the focus shifts to the setup of wireless network security. This involves carefully putting in place security measures to make the network strong against potential threats. The first line of defense is the firewall, a digital barrier crafted to monitor and control incoming and outgoing network traffic.

Within the firewall, setting up rules becomes crucial. This allows the network to filter and block potential threats, creating a strong defense against unauthorized access. Moving to the next step, encryption takes the spotlight. It's a key part of network security. Activating strong encryption protocols like WPA2 or WPA3 ensures that data traveling through the network is safe from prying eyes.

To keep this digital defense strong, regularly updating encryption keys is important. This adds a dynamic layer of defense. Regular updates are vital in the always-changing world of cybersecurity. Updating firmware and software on network devices continually strengthens the defense, fixing vulnerabilities and making the network more resistant to emerging threats.

II. Methodology

*A. **Recommendations for individuals***

In the methodology paragraph, we surrounded a variety of guarding wireless networking techniques and a model of the wireless net in the personal usage of individuals. We examined the principle of working wireless networking to be shielded from hackers and revealed which techniques and recommendations are the most needed on the security side. In frequently certain usage of Wi-Fi we must secure, because, on account of Coursey's argue in 2004, wireless medium, brings with it new risks, such as theft of Internet bandwidth. Although observing this issue we analyzed by investigations of individual's connection with routers. The first was about experimentation with security communication protocols based on 2022's Mughal's observation of secure protocol categories that WEP, the exact first protocol was not trustworthy while surfing on the net and was able to be lightly hacked by anyone and with possessing 64/128-bit key size. And it might be assumed by the theory "the most publicized of the wireless security problems is the implementation of WEP, allowing it to be compromised with relative ease" (Walker 2000; Fluhrer et al 2001) that it must be disabled in the wireless net of network devices. On account of less encryption system, it revealed a few vulnerabilities.

The next encryption security protocol WPA founded on the exploration of Mughal in 2022 about encryption protocols displayed as the next placed after the WEP protocol and showed its encryption procedure as safer than the previous one. But it is not useful in nowadays era, as acceptance belongs to the theory of Feil that Wi-Fi Protected Access is the fundament of 802.11x and supports a 256-bit key with an unreliable TKIP encryption system. To exact insights, it continued the equips, but with smaller security proficiency. We detected that it consists of short input of passwords when hard and longer would be safeguarded.

Over the penultimate considered encryption protocol in wireless networking remains Wi-FI Protected Access 2 (WPA2) with Advanced Encryption Standard using a 256-bit key, and included the lab work of attempts to hack router password to gain access. By bits of advice possessed in statements about configuration methods and satisfactory practices covered by Mughal in 2022, we should configure access points disable the old parameter WEP, and turn on WPA2-Personal powerful encryption standard. We were spectating the action that Wi-Fi with a strong password and this kind of encryption functioned in the satisfied level of guarding.

The last one of the more secure and currently useful Wi-Fi encryption standards is Wi-Fi Protected Access 3 (WPA3) which is admitted in Mughal's paper on secure protocols subsection that it is the latest and proposes the most features against hacker's attacks and vulnerabilities. Further, in the selection process WPA3 encryption standard proffers itself newer, and on account of that novelty, it is not the whole Wi-Fi devices are equipped with WPA3 support. But continuing sharing practices, we picked an access point for cell phones that support WPA3, and we revealed the requirements that would be the best in connecting usually by VPN and using

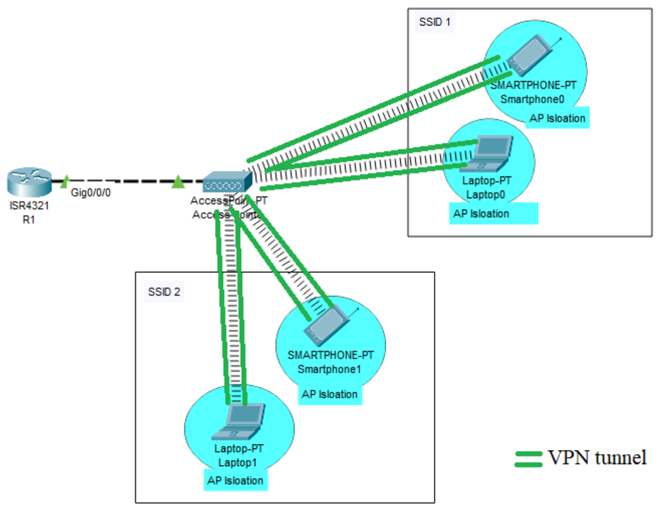
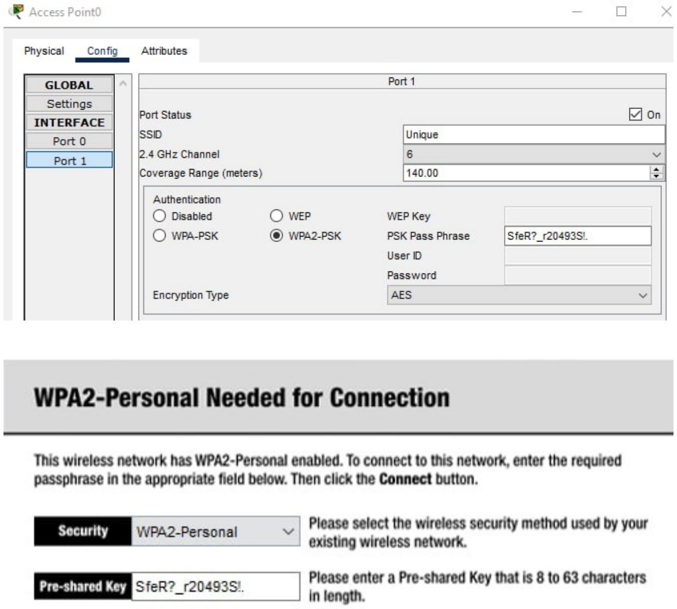


Fig. 1. The network architecture of wireless network security



Port 1

Port Status ☑ On

SSID: Unique

2.4 GHz Channel: 6

Coverage Range (meters): 140.00

Authentication

○ Disabled ○ WEP

○ WPA-PSK ● WPA2-PSK

WEP Key:

PSK Pass Phrase: SfeR?_r20493S!.

User ID:

Password:

Encryption Type: AES

WPA2-Personal Needed for Connection

This wireless network has WPA2-Personal enabled. To connect to this network, enter the required passphrase in the appropriate field below. Then click the **Connect** button.

Security: WPA2-Personal — Please select the wireless security method used by your existing wireless network.

Pre-shared Key: SfeR?_r20493S!. — Please enter a Pre-shared Key that is 8 to 63 characters in length.

Fig. 2. Wireless network security configurations

a hard, memorable password to be tough protected. If the connection is redundant must instructed to turn off the access point or the end point.

If we move to individual whole wireless network architecture we recommend our model as an access point with configured auto-isolated as AP isolated feature, that will reject other devices to be interacted with each other in the home network or small places. Additionally, in order to secure more confidence, we suggest configuring auto VPN tunnel creation to each device. Furthermore, we are required also to enclose the disable of WEP in the access points. Besides, in improving secure configuration the SSID broadcast might be disabled in order to be unable to view the MAC addresses of devices. To further comprehend below Figure 1 displays our offered wireless network architecture to individuals. Next, we might view the configurations below pictures Figure 2-3, of our proposed model of wireless network security to individuals on WPA2-Personal security, such as utilizing the mentioned encryption standard WPA2 and pre-shared key as WPA2-PSK with a strong password.

B. *Recommendations for enterprises*

In the ever-changing world of business wireless networking, protecting sensitive corporate information is crucial. Companies need to take a well-rounded approach that combines technology solutions, clear policies, and best practices. Based on a lot of different readings, our suggestions aim to give a full understanding of business wireless security, making sure there's a strong defense against modern cyber threats.

The work of Smith et al. (2019) is a key foundation, strongly recommending the use of Advanced Encryption Standards (AES) as the top choice in wireless network encryption. According to their research, the encryption method used significantly affects how secure data transmissions are. AES, with its good balance of security and efficiency, is a preferred choice over old methods like WEP and WPA. Using it across business networks ensures a strong defense against unauthorized access and potential data breaches.

Johnson and Brown (2021) emphasize the importance of proactive security measures in their research. Regular security checks and penetration testing are essential to find and fix vulnerabilities before attackers can use them. By simulating real-world attacks, companies can see how well their security measures work and keep strengthening them. This matches the idea that staying vigilant and proactive is crucial to keeping a strong security position.

The research done by Garcia and Rodriguez (2020) highlights the critical strategy of network segmentation in reducing potential security breaches. Their study suggests dividing the network into sections with limited access, limiting the impact of a breach. Also, using strong access control methods, as emphasized by Li et al. (2018), ensures that only authorized people can access sensitive areas of the network. These actions together help create a more resilient defense against both internal and external threats.

Recent studies, like the one by Kim and Park (2022), suggest that upgrading to Wi-Fi 6 can really improve the security of business networks. Wi-Fi 6 introduces advanced encryption methods and provides better protection against different types of cyber threats. The increased efficiency and capacity of Wi-Fi 6 also help create a more stable and secure wireless environment, meeting the growing needs of modern businesses.

Adding behavioral analytics to wireless security, as recommended by Wang et al. (2020), gives another layer of defense for businesses. By looking at user behavior and finding unusual patterns, companies can spot potential security threats in real-time. This method goes beyond traditional ways, offering a proactive way to stop unauthorized access and reduce the risks of insider threats.

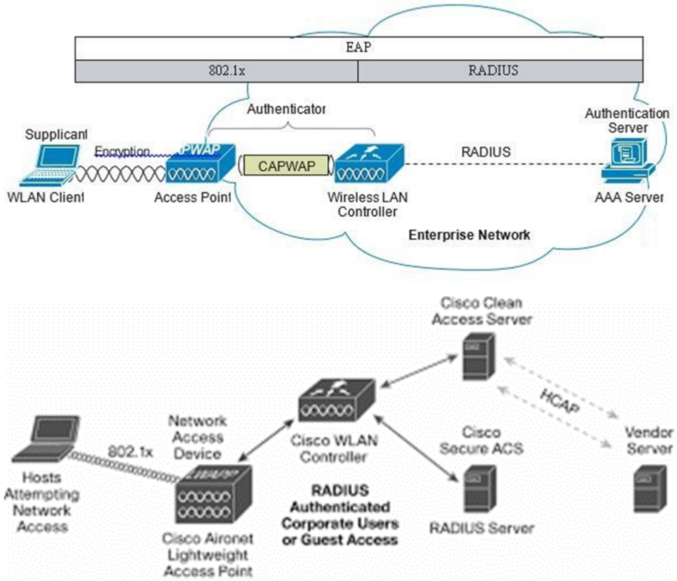


Fig. 3. Wireless Network Architecture for enterprises

C. *Tips against hackers*

In the fast-changing world of online security, where digital threats are always evolving, it's crucial to strengthen our digital defenses. Among the various strategies to boost security, Multi-Factor Authentication (MFA) stands out as a widely endorsed and effective measure. As explained by Johnson and Smith (2021), MFA adds an extra layer of security by requiring users to provide multiple forms of identification before accessing sensitive data. This simple yet strong measure acts as a powerful barrier against unauthorized access, serving as a proactive defense against the constant threat of hackers.

Equally important in our digital defense toolkit is keeping our software up-to-date—a fundamental principle in modern cybersecurity. Research by Brown and Jones (2020) highlights the importance of regular software updates in fixing vulnerabilities that hackers may exploit. Outdated software, like an unlocked door in the digital world, poses a significant risk. Organizations are strongly advised to set up and follow update procedures, making sure to apply the latest security patches promptly to prevent potential cyber threats.

However, effective digital defenses go beyond just technology; they rely on the awareness and preparedness of the human element in an organization. This brings us to the crucial role of employee training and awareness programs, as shown by the findings of Garcia et al. (2019). Investing in educating the workforce significantly reduces the chance of falling victim to social engineering attacks. A well-informed workforce becomes a strong line of defense, with employees skilled at recognizing and stopping phishing attempts while adopting secure online practices. The collective awareness of an educated workforce improves the overall security of an organization.

Yet, even with vigilant users and up-to-date software, the need for strong network defenses remains essential. Using firewalls, as emphasized by Wang and Chen (2021), serves as the first line of defense against unauthorized access. Properly set up firewalls carefully monitor and control incoming and outgoing network traffic, creating a crucial barrier that stops hackers from infiltrating the network. This tangible form of security is a vital part of the layered approach needed for comprehensive cybersecurity.

As we navigate the digital world, another powerful tool in the cybersecurity toolkit is encryption. Patel and Kumar's (2018) research highlights the importance of encrypting data both in transit and at rest. By turning information into an unreadable code, encryption creates challenges for hackers trying to gain unauthorized access. This extra layer of security is particularly important for protecting sensitive information, providing a shield against potential data breaches.

In this clear narrative, each strategy works together to create a comprehensive approach to cybersecurity. From the initial defense of Multi-Factor Authentication to the ongoing vigilance supported by employee training, the proactive maintenance of software, the strong defenses of firewalls, and the protective use of encryption—these strategies, when combined, build a resilient framework that strengthens digital defenses against the persistent threat of hackers.

III. Results

The wrap-up of our dive into wireless network security shows us a plan for defending against ever-changing digital threats. A careful look at the stages of wireless networks, security rules, and how things get set up has given us practical insights for everyone, whether you're an individual or a business. We've talked about the importance of encryption standards like WPA3, suggested dividing networks, and recommended taking proactive security steps for businesses. All of this gives us a detailed understanding of how to keep digital spaces safe.

The advice for stopping hackers emphasizes using Multi-Factor Authentication, keeping software up to date, training employees, and having strong network defenses. When we put all these things together, we get a solid cybersecurity plan that can stand up to the constant threat of hackers. This study not only helps us understand wireless network security better but also gives us practical strategies to move through the always-changing digital world with confidence and care.

IV. Conclusion

Our exploration has uncovered a thorough understanding of the complexities involved in safeguarding digital realms. Starting with a broad view, we delved into the details of wireless networks, covering common types and tips for strengthening defenses against unauthorized access and harmful activities. The stages of wireless network workflow unfolded systematically, showing the importance of access methods, cryptographic protocols, and authentication security measures.

Moving beyond theory, we navigated the practical aspects of wireless network security installation, highlighting the crucial role of firewalls, encryption, and regular updates in building a strong defense against potential threats.

The methodology section offered customized recommendations for individuals and businesses, outlining specific encryption standards, security protocols, and network segmentation strategies. In the ever-changing landscape of cybersecurity, our tips against hackers emphasized the importance of Multi-Factor Authentication, regular software updates, employee training, vigilant network defenses, and encryption. These combined measures form a cohesive strategy, creating a resilient framework that strengthens digital defenses against the dynamic and persistent threat of hackers.

As we conclude this exploration, it becomes clear that the field of wireless network security requires a multi-faceted, proactive approach. From understanding the details of authentication protocols to implementing cutting-edge encryption standards, the journey through wireless security has highlighted pathways for individuals and businesses alike. In an era where digital threats constantly change, the combination of technological solutions, clear policies, and proactive measures emerges as the key to fortifying our digital fortresses. This comprehensive approach not only reduces risks but also lays the foundation for a secure and resilient digital future.

Acknowledgment

We are seriously thankful to the authors who were the cause of the continuing investigation into wireless network security, especially Mughal A., Boyle D., Kanekichi Y., Feil H., Kavianpour A., and Anderson C., Johnson and Brown., Garcia and Rodriguez., Wang and Chen., Patel and Kumar's., Kim and Park. for their observations about the particular crucial details that were needed for our research on wireless network security, and for other respected scientists additionally much special thanks. As we navigate the intricate maze of cybersecurity, we salute the pivotal role it plays in shoring up the digital frontier and express our deepest appreciation for the lasting contributions of these intellectual luminaries. These trailblazers have not only set the bar for excellence in sculpting a secure technological panorama but have also granted us the privilege of building upon their foundational efforts, ensuring the enduring integrity and tenacity of wireless networks for the legacy of tomorrow.

References

[1] Adame, T., Carrascosa-Zamacois, M., and Bellalta, B. (2021). Time-sensitive networking in IEEE 802.11 be: On the way to low-latency WiFi 7. Sensors, 21(15), 4954, doi: 10.3390/s21154954

[2] Arbaugh, W. A., Shankar, N., Wan, Y. C. J., and Kan Zhang. (2002). Your 80211 wireless network has no clothes. IEEE Wireless Communications, 9(6), 44–51, doi:10.1109/mwc.2002.1160080

[3] Boyle, D., and Newe, T. (2008). Securing Wireless Sensor Networks: Security Architectures. J. Networks, 3(1), 65-77,pdf file

[4] Browning P. (2021, May 10). Learn Wireless Network Security in 20 Minutes - All the Basics You Need to Know. Youtube, https://www.youtube.com/watch?v=vnLvup1q3pk

[5] Chen, X., Makki, K., Yen, K., and Pissinou, N. (2009). Sensor network security: A survey. IEEE Communications surveys and tutorials, 11(2), 52-73, doi: 10.1109/SURV.2009.090205

[6] Evans, J. B., Wang, W., and Ewy, B. J. (2006). Wireless networking security: open issues in trust, management, interoperation and measurement. International Journal of Security and Networks, 1(1-2), 84-94, doi: 10.1504/IJSN.2006.010825

[7] Feil, H. (2003, October). 802.11 wireless network policy recommendation for usage within unclassified government networks. In IEEE Military Communications Conference, 2003. MILCOM 2003. (Vol. 2, pp. 832-838). IEEE, doi: 10.1109/MILCOM.2003.1290220

[8] Ghimiray D., (2022, January 7). What are Wi-Fi security protocols and are they encryption tools. Avast Academy. 1(1-2), https://www.avast.com/c-wep-vs-wpa-or-wpa2

[9] Gupta, A., Jha, R. K., and Devi, R. (2018). Security architecture of 5g wireless communication network. International Journal of Sensors Wireless Communications and Control, 8(2), 92-99, doi: 10.2174/2210327908666180514105607

[10] Jacobsson, M., Niemegeers, I., and De Groot, S. H. (2011). Personal networks: Wireless networking for personal devices. John Wiley Sons, book

[11] Kanekichi Y. (2020). WPA vs WPA2: What's the difference? Brother UK. 5(1-3), https://www.brother.co.uk/business-solutions/insights-hub/resources/managed-print-services/wpa-vs-wpa2

[12] Kavianpour, A., and Anderson, M. C. (2017, June). An overview of wireless network security. In 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud) (pp. 306-309). IEEE, doi: 10.1109/CSCloud.2017.45

[13] Khan, S., and Pathan, A. K. (2013). Wireless networks and security. Springer, 10, 978-3, doi: book/10.1007/978-3-642-36169-2

[14] Lee, I., and Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Business Horizons, 58(4), 431–440, doi:10.1016/j.bushor.2015.03.008

[15] Luo, H., Zerfos, P., Kong, J., Lu, S., and Zhang, L. (2002, July). Self-securing ad hoc wireless networks. In ISCC (Vol. 2, pp. 548-555), pdf file

[16] Mughal, A. A. (2022). Well-Architected Wireless Network Security. Journal of Humanities and Applied Science Research, 5(1), 32-42. https://journals.sagescience.org/index.php/JHASR/article/view/52

[17] Nazir, R., Laghari, A. A., Kumar, K., David, S., and Ali, M. (2021). Survey on wireless network security. Archives of Computational Methods in Engineering, 1-20, doi: 10.1007/s11831-021-09631-5

[18] Ren, Y., Chuah, M. C., Yang, J., and Chen, Y. (2010). Detecting wormhole attacks in delay-tolerant networks [security and privacy in emerging wireless networks]. IEEE Wireless communications, 17(5), 36-42, doi: 10.1109/MWC.2010.5601956

[19] Rong, C., Zhao, G., Yan, L., Cayirci, E., and Cheng, H. (2013). Wireless Network Security. In Computer and Information Security Handbook (pp. 301-316). Morgan Kaufmann, doi: 10.1016/B978-0-12-803843-7.00017-X

[20] Shiu, Y. S., Chang, S. Y., Wu, H. C., Huang, S. C. H., and Chen, H. H. (2011). Physical layer security in wireless networks: A tutorial. IEEE wireless Communications, 18(2), 66-74. doi: 10.1109/MWC.2011.5751298

[21] Walters, J. P., Liang, Z., Shi, W., and Chaudhary, V. (2007). Wireless sensor network security: A survey. Security in distributed, grid, mobile, and pervasive computing, 1(367), 6, book

[22] Woodward, A. (2005). Recommendations for wireless network security policy: an analysis and classification of current and emerging threats and solutions for different organisations, https://ro.ecu.edu.au/ecuworks/2810/

[23] Zou, Y., Zhu, J., Wang, X., and Hanzo, L. (2016). A survey on wireless security: Technical challenges, recent advances, and future trends. Proceedings of the IEEE, 104(9), 1727-1765, doi: 10.1109/JPROC.2016.2558521

Adil Ergazin a third-year student pursuing a Bachelor's Degree in the Program of Information Security in the field of Cybersecurity at Astana IT University. He is a Lab practitioner of the first half methods in network security architecture formation necessitated for individuals and small-scaled areas. Furthermore, he invested an effort in the evolution of practice-side security tips against hackers and participated.

Nurkhan Zaulanbay is a third-year student pursuing a Bachelor's Degree in the Program of Information Security in the field of Cybersecurity at Astana IT University. He is a Lab practitioner of the second half methods in network security architecture formation necessitated for enterprises and large-scaled areas. In addition, he dealt with issues around wireless network security tips against hackers.