JERIT: Journal of Educational Research and Innovation Technology
Homepage: https://jerit.unimika.ac.id/index.php/jerit
Email: jeritunimika@gmail.com

e-ISSN: 3063-5462
Vol. 2, No. 2, December 2025
Page 73-82

WIRELESS FIDELITY NETWORK SECURITY THREATS (Wi-Fi)

Irfan Zulkarnaen[1], M Ziran Maulana R[2], Syarifudin[3], Sebastian Rinaldi[4], Umar Akem[5]
[1*,2,3,4] Sekolah Tinggi Teknologi Wastukancana Purwakarta, Indonesia
[5] Ibnu Auf Technological College, Thailand

Email: irfanzulkarnaen02@wastukancana.ac.id

ABSTRACT

The advancement of wireless network technology has improved communication efficiency but also increased the risk of data security breaches. One significant threat to Wi-Fi networks is the use of tools like Nethercap to conduct Man-in-the-Middle (MitM) attacks. This study aims to explore in depth how Nethercap is used to steal Wi-Fi credentials, evaluate its impact on information security, and propose mitigation strategies. However, the convenience and flexibility offered by WiFi does not come without risks. Due to its radio wave-based nature and wide signal spread, WiFi networks are vulnerable to various security threats. In many cases, users or network administrators often neglect security aspects or are unaware of loopholes that could be exploited by malicious parties. As a result, sensitive information can be leaked, illegal access to the network can be gained, or even malicious activities can be carried out through a compromised network. Therefore, it is very important for anyone who manages or uses a WiFi network to understand the types of threats that may occur and implement appropriate solutions to maintain network security. The research method employed is descriptive qualitative with a case study approach. The analysis results show that Nethercap exploits vulnerabilities in wireless protocols, potentially leading to data theft, privacy violations, and organizational losses. Mitigation strategies include the implementation of WPA3, network segmentation, deployment of SIEM systems, and enhanced cybersecurity awareness.

Keywords: Nethercap, Wi-Fi, Network Security, MitM, WPA3, Encryption, Cyber Attacks

***Corresponding Author:** juniawanmp@gmail.com
Received: August 7th 2025; Revised: August 21th 2025; Accepted: November 26th 2025
DOI: https://doi.org/10.34125/jerit.v2i2.26

Reference to this paper should be made as follows: Putra, J.M., Menorizah, M. Wireless Fidelity Network Security Threats (Wi-Fi). *JERIT: Journal of Educational Research and Innovation Technology, 2* (2), 73-82.
E-ISSN: 3063-5462
Published by: JERIT: Journal of Educational Research and Innovation Technology

INTRODUCTION

In this increasingly connected digital era, Wireless Fidelity (Wi-Fi) networks have become the primary backbone of communication and data exchange across various sectors, from education and business to government and even households. Wi-Fi enables unlimited internet access through efficient, practical, and cost-effective wireless connectivity.

However, behind this convenience, there are various network security threats that have the potential to cause significant losses, both financially and privacy-wise. These threats include attacks such as Man-in-the-Middle (MITM)., Evil Twin Attack, Packet Sniffing, Denial of Service (DoS), to theft of user credentials (Andress, 2024). One of the main problems with Wi-Fi networks is their open nature and Easily accessible, making it easier for attackers to exploit weaknesses in security systems. According to research by Alotaibi & El-Alfy (2021) in IEEE Access, attacks on Wi-Fi networks have increased significantly with the growth of Internet of Things (IoT) devices, which often have weak security systems. This expands the attack surface that can be exploited by malicious parties to steal sensitive data or compromise network systems (Baroud et al, 2024).

Furthermore, many public Wi-Fi users—such as those in cafes, airports, and universities—lack awareness of cybersecurity risks. They often access banking services or send personal information without adequate encryption protection. According to a report from Kaspersky Security Bulletin (2023), more than 60% of global internet users still use public networks without a Virtual Private Network (VPN), leaving their data vulnerable to theft. This situation highlights the need for increased awareness and the implementation of stronger network security technologies (Iskandar et al, 2022).

Various solutions have been developed to address these threats. One key approach is the use of updated security protocols, such as WPA3, which offers stronger encryption and protection against brute-force attacks. Additionally, the implementation of multi-factor authentication systems And A Virtual Private Network (VPN) can provide an additional layer of security for users. The use of an adaptive firewall, Intrusion Detection System (IDS), as well as Intrusion Prevention System (IPS) can also help detect and prevent suspicious activity on Wi-Fi networks (Kim JH et al, 2021).

Furthermore, artificial intelligence (AI) and machine learning-based approaches are increasingly being used in modern network security systems. This technology can analyze data traffic patterns in real time and identify anomalies that indicate cyberattacks. Research by Ahmed et al. (2022) in the Journal of Network and Computer Applications shows that AI-based intrusion detection models can improve threat identification accuracy by up to 95% compared to traditional systems.

Therefore, solutions to Wi-Fi network threats depend not only on technical aspects but also on personal data. Education about digital security practices, regular software updates, and the implementation of appropriate security protocols are essential steps to creating a more secure network. With a combination of advanced technology and wise user behavior, threats to Wi-Fi networks can be significantly minimized (Septiani et al, 2024).

The rapid development of information and communication technology in the digital era has brought about major transformations in various sectors, including education, industry, government, and social life. One important component of this digital infrastructure is wireless networks (Wi-Fi), which provide easy connectivity and high

mobility for its users. However, behind this convenience, Wi-Fi networks also present significant challenges in terms of data and information security. Data security is a crucial issue because information has become a highly valuable strategic asset, both for individuals and organizations. Information security breaches can have serious consequences, ranging from personal data theft, financial losses, to disruptions to organizational operations. One real threat in the context of Wi-Fi networks is the use of hacking tools such as Nethercap, an open-source software capable of carrying out Man-in-the-Middle (MitM) attacks, packet sniffing, and unauthorized user credential harvesting (Laudon et al, 2020).

These threats are becoming increasingly relevant given the low level of digital security awareness among users and the weak protection of many Wi-Fi networks, particularly those still using outdated encryption standards. Nethercap and similar tools create significant opportunities for cybercriminals to exploit data transmitted over unprotected networks. This research aims to examine how Nethercap works as a Wi-Fi attack tool, analyze the risks it poses to data security, and evaluate potential mitigation strategies. Using a descriptive qualitative approach, this study aims to provide a deeper understanding of the threat characteristics and relevant defense solutions, both in individual and organizational contexts (Whitman et al, 2017).

METHODS

This study uses a descriptive qualitative approach to in-depth examine the characteristics, working methods, and impacts of the Nethercap tool in the context of wireless network (Wi-Fi) security. This approach was chosen because it is suitable for explaining phenomena in a contextual and exploratory manner, especially for research objects that have not been widely discussed in previous studies. Qualitative methods are used to gain a comprehensive understanding of the Nethercap tool as a threat to information security. The main focus of this study is to observe and explain the Nethercap working process, the attack techniques used, and its impact on the Confidentiality, Integrity, and Availability (CIA Triad) aspects of information systems (Koonteko et al, 2013).

Table 2. Research Method Data

Research Title	Security Approach	Advantages	Disadvantages
Social Engineering: Deauther & Evil Twin	Social prevention through education and SSID management	Focus on increasing user awareness	Does not involve in-depth technical mitigation
Phishing with ESP8266	Social engineering simulation and captive portal	Depicting real threats on the ground	The solution is only a recommendation, not a systematic one.
Packet Sniffing Analysis	Network traffic analysis using sniffing tools	Providing solutions such as	Less focus on modern tools like Nethercap

		segmentation and encryption	
Wardriving dan Wifiphishe	Wardriving techniques to identify public Wi-Fi vulnerabilities	Valid for public Wi-Fi	Not yet discussing industry standards-based mitigation

Data Collection Techniques

Data collection is carried out through three main techniques:

a) Literature Review: References are taken from academic books, scientific journals, international standards (such as ISO/IEC 27001), as well as technical documents from cybersecurity vendors (Kaspersky, Symantec, NIST).
b) Simulation Observation: The author conducted observations of Nethercap's work processes in a limited virtual environment with educational and exploratory purposes, without harming other parties.
c) Case Study Analysis: Using Nethercap as a study object to identify risks and potential threats to Wi-Fi networks in both general user and organizational environments.

Data Analysis Techniques

The data obtained were analyzed thematically and narratively, to identify:

a) Attack patterns carried out by Nethercap
b) Wi-Fi network system vulnerabilities
c) Mitigation strategies that can be implemented

In addition, a risk analysis approach and evaluation of compliance with information security standards, such as ISO/IEC 27001 and national regulations (UU ITE, PP PSTE), are carried out to understand policy and technical gaps that can be exploited by attackers.

RESULTS AND DISCUSSION

The Threat of Nethercap

Nethercap is a highly effective tool for conducting Man-in-the-Middle (MitM) attacks. Here's a flowchart of a Nethercap attack on a Wi-Fi network:

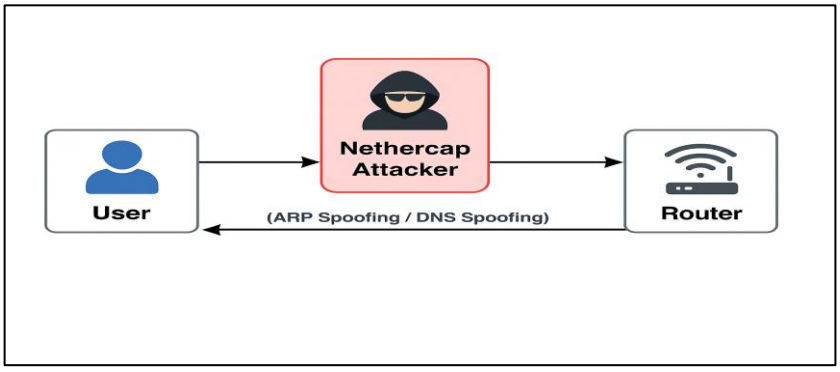

Figure 1. Attackers Infiltrate Between User and Router Communications, Stealing Transmitted Data Such as Passwords and Login Data

Identifying Wi-Fi Network Security Threats

Nethercap is a hacking tool that can be used to perform various attack techniques on Wi-Fi networks, such as Man-in-the-Middle (MitM), packet sniffing, ARP spoofing, and creating fake captive portals. These techniques allow attackers to access sensitive data transmitted over the network, such as usernames, passwords, and other personal information.

This tool works by exploiting vulnerabilities in Wi-Fi networks, particularly those protocols that still use legacy encryption systems (e.g., WEP or WPA). In simulations, Nethercap successfully redirected victim traffic to a fake network and secretly recorded authentication data.

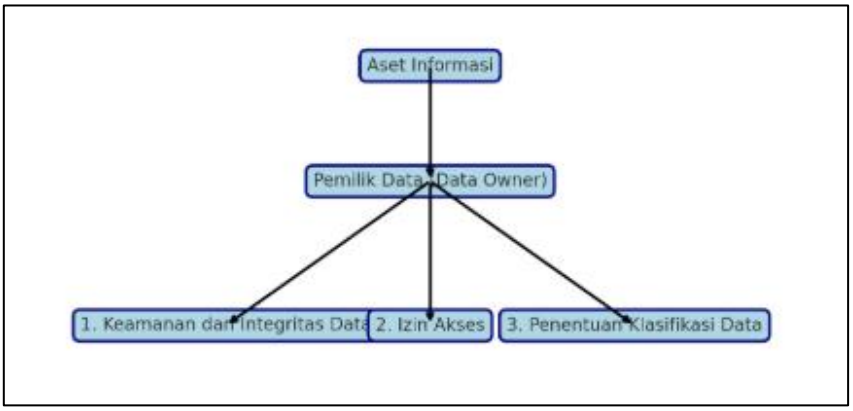

Figure 2. Ownership mapping

Risk and Vulnerability Analysis

Observation results show several vulnerabilities that are often found in Wi-Fi networks:

a) Use of weak or default passwords
b) No network traffic monitoring
c) User ignorance of the threat of fake access points
d) The absence of an intrusion detection system (IDS) or SIEM

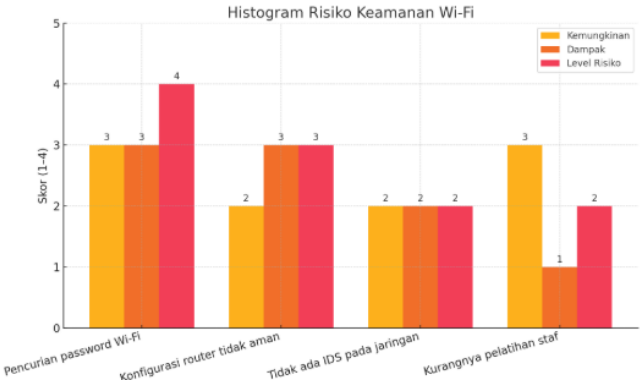

Figure 4. Histogram of levels and levels

Below is a histogram comparing the likelihood, impact, and risk levels of each Wi-Fi security threat scenario. The values are converted to a numeric scale (1–4) for visualization:

1: Low
2: Medium

3: High
4: Extreme

The risk of this attack is extremely high. If Wi-Fi credentials are successfully stolen, attackers can gain access to an organization's internal network, spread malware, steal data, and even access production systems. The following is a summary of the effectiveness of each encryption type in preventing attacks like Nethercap's, based on literature studies and simulations:

Table 2. Effectiveness of each type of encryption

Encryption Types	Security Level	Vulnerable to Nethercap
WEP	Low	Very Vulnerable
WPA	Secondary	Prone to
WPA2	High	Relatively Safe
WPA3	Very high	Hard to Exploit

Evaluation of Compliance with Security Standards

From an assessment of the ISO/IEC 27001 standard and national regulations (ITE Law), many organizations have not implemented basic controls such as:

a) Strict access control policy (A.9)
b) Malware protection system (A.12)
c) Routine security audits (A.18)

Compliance analysis shows that organizations that do not harden their Wi-Fi networks may be considered negligent and risk legal penalties in the event of a data breach.

Mitigation Strategy

Some suggested mitigation strategies to protect networks from Nethercap attacks include:

a) Using WPA3 encryption: Provides stronger protection than WPA/WEP.
b) Network segmentation: Separating guest and internal networks to limit attackers' room for maneuver.
c) SIEM and IDS/IPS Implementation: Detect and respond to suspicious activity in real-time.
d) Cybersecurity education: Raising user awareness to not carelessly connect to Wi-Fi networks.

CONCLUSION

This study examines threats to Wi-Fi network security with a focus on the Nethercap hacking tool. Based on the analysis, it can be concluded that attacks on wireless networks, particularly through Man-in-the-Middle (MitM) techniques, are a dangerous form of attack and are increasingly easy to carry out with the availability of open-source tools such as Nethercap. Weak Wi-Fi network security, especially those that still use WEP/WPA encryption or do not implement network segmentation, is highly vulnerable to exploitation by irresponsible parties. Furthermore, a lack of user awareness and weak organizational policies exacerbate the risk of data leakage.

Nethercap is a Linux-based hacking tool used to conduct MitM attacks through techniques such as ARP spoofing, DNS spoofing, and packet sniffing to steal Wi-Fi credentials and personal user data. The impact of using Nethercap is significant, such as information theft, unauthorized access to the network, privacy violations, and potential financial and reputational losses, especially for organizations that do not implement adequate security systems. Nethercap violates the CIA Triad (Confidentiality, Integrity, Availability), a fundamental principle in information security, as it allows attackers to read, modify, or intercept network traffic. Many organizations are still not fully compliant with information security standards, such as ISO/IEC 27001 and national regulations (such as the ITE Law), especially regarding access control, network monitoring, and security audits. Mitigating Nethercap attacks requires a layered security approach, such as the use of WPA3 encryption, network segmentation (VLANs), the use of SIEM and IDS/IPS systems, and cybersecurity literacy campaigns to raise user awareness. By understanding the workings and risks of the Nethercap tool, organizations and individuals can increase their vigilance and take strategic steps to protect the integrity and security of their wireless network systems.

ACKNOWLEDGEMENTS

The author would like to thank the lecturer in charge of the Data and Information Security course, Mr. M. Agus Sunandar, S.T., M.Kom, who has provided guidance, direction, and motivation in the process of compiling this journal. Thanks are also extended to his teammates for their cooperation and contributions during the research and writing process. The author also appreciates the various parties who have provided references and literature sources that serve as the basis for the analysis and development of the contents of this journal. Hopefully, this journal can make a positive contribution in increasing awareness and knowledge about network security, especially in dealing with Wi-Fi-based cyber threats such as Nethercap.

REFERENCE

Andress, J. (2019). *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice* (3rd ed.). Elsevier.

Amrulloh, N. M. A. G. (2024). Educator Recruitment Management in Improving Student Quality at Dwiwarna Parung High School. *JERIT: Journal of Educational Research and Innovation Technology*, *1*(2), 80–90. https://doi.org/10.34125/jerit.v1i2.9

Amir, A., Afnita, A., Zuve, F. O., & Erlianti, G. (2024). Education and Application of Digital Media in Creation and Documentation Artery Based Service Letter. *JERIT: Journal of Educational Research and Innovation Technology*, *1*(1), 36–42. https://doi.org/10.34125/jerit.v1i1.5

Adeoye, M. A., & Otemuyiwa, B. I. (2024). Navigating the Future: Strategies of EdTech Companies in Driving Educational Transformation. *JERIT: Journal of Educational Research and Innovation Technology*, *1*(1), 43–50. https://doi.org/10.34125/jerit.v1i1.10

Arifianto, A., & Purnomo, M. S. (2024). The Role of Marketing Management in The Development of Islamic Education Services. *JERIT: Journal of Educational*

Research and Innovation Technology, *1*(2), 112–122. https://doi.org/10.34125/jerit.v1i2.14

Adeoye, M. A., Obi, S. N., Sulaimon, J. T., & Yusuf, J. (2025). Navigating the Digital Era: AI's Influence on Educational Quality Management. *JERIT: Journal of Educational Research and Innovation Technology*, *2*(1), 14–27. https://doi.org/10.34125/jerit.v2i1.18

Anwar, C., Septiani, D., & Riva'i, F. A. (2024). Implementation Of Curriculum Management Of Tahfidz Al-Qur'an at Al-Qur'an Islamiyah Bandung Elementary School. *INJIES: Journal of Islamic Education Studies*, *1*(2), 91–96. https://doi.org/10.34125/injies.v1i2.11

Ayuba, J. O., Abdulkadir, S., & Mohammed, A. A. (2025). Integration of Digital Tools for Teaching and Learning of Islamic Studies Among Senior Secondary Schools in Ilorin Metropolis, Nigeria. *INJIES: Journal of Islamic Education Studies*, *2*(1), 1–9. https://doi.org/10.34125/injies.v2i1.16

Ayuba, J. O., Abdullateef, L. A., & Mutathahirin, M. (2025). Assessing the Utilization of Information and Communication Technology (ICT) Tools for Teaching Secondary Schools Islamic Studies in Ilorin, Nigeria. *JERIT: Journal of Educational Research and Innovation Technology*, *2*(1), 28–37. https://doi.org/10.34125/jerit.v2i1.22

Alwaan, A. Z., & T, N. A. (2024). Dakwah Strategy in The Modern Era. *INJIES: Journal of Islamic Education Studies*, *1*(1), 28–34. https://doi.org/10.34125/injies.v1i1.4

Aziz, M., 'Arif, M., Alwi, M. F., & Nugraha, M. N. (2024). Improving The Quality of Education Through Optimizing the Educational Administration System at The An-Nur Islamic Education Foundation. *INJIES: Journal of Islamic Education Studies*, *1*(1), 5–15. https://doi.org/10.34125/injies.v1i1.2

Abiyusuf, I., Hafizi, M., Pakhrurrozi, P., Saputra, W., & Hermanto, E. (2024). Critical Analysis of The Rejection of Richard Bell's Thoughts on The Translation of The Qur'an in The Context of Orientalism. *INJIES: Journal of Islamic Education Studies*, *1*(2), 48–60. https://doi.org/10.34125/injies.v1i2.6

Baroud, N., Alouzi, K., Elfzzani, Z., Ayad, N., & Albshkar, H. (2024). Educators' Perspectives on Using (AI) As A Content Creation Tool in Libyan Higher Education: A Case Study of The University of Zawia. *JERIT: Journal of Educational Research and Innovation Technology*, *1*(2), 61–70. https://doi.org/10.34125/jerit.v1i2.12

Bejtlich, R. (2014). *The Practice of Network Security Monitoring: Understanding Incident Detection and Response*. No Starch Press.

Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (4th ed.). SAGE Publications.

GDPR. (2018). *General Data Protection Regulation*. Retrieved from https://gdpr.eu

Hidayatullah, R. R., Kamali, M. F., & T,. N. A. (2024). Innovative Dakwah Strategies Through Social Media: Case Study of Islamic Communication Approaches in Indonesia. *INJIES: Journal of Islamic Education Studies*, *1*(1), 16–27. https://doi.org/10.34125/injies.v1i1.3

Hidayati, E., & Hutagaol, B. A.-R. (2025). An Analysis of Hasan Hanafi's Tafsir Method: Hermeneutics as An Interpretative Approach. *INJIES: Journal of Islamic Education Studies*, *2*(1), 39–48. https://doi.org/10.34125/injies.v2i1.22

Iskandar, M. Y., Nugraha, R. A., Halimahturrafiah, N., Amarullah, T. A. H., & Putra, D. A. (2024). Development of Android-Based Digital Pocketbook Learning Media in Pancasila and Citizenship Education Subjects For Class VIII SMP . *JERIT: Journal of Educational Research and Innovation Technology*, *1*(2), 51–60. https://doi.org/10.34125/jerit.v1i2.13

Islam, I., & Ishaq, M. (2024). Development of Journalism Development Strategies in The Digital Era at Darul Mukhlasin High School. *JERIT: Journal of Educational Research and Innovation Technology*, *1*(2), 71–79. https://doi.org/10.34125/jerit.v1i2.11

ISO/IEC. (2013). *ISO/IEC 27001: Information Security Management Systems – Requirements*. International Organization for Standardization.

ISO/IEC. (2018). *ISO/IEC 27005: Information Security Risk Management*. International Organization for Standardization.

Iswandi, I., Syarnubi, S., Rahmawati, U., Lutfiyani, L., & Hamrah, D. (2024). The Role of Professional Ethics Courses in Producing Prospective Islamic Religious Education Teachers with Character. *INJIES: Journal of Islamic Education Studies*, *1*(2), 71–82. https://doi.org/10.34125/injies.v1i2.9

Khofi, M. B., & Santoso, S. (2024). Optimize the Role of The State Islamic High School (MAN) Bondowoso Principal in Promoting Digital-Based Learning. *JERIT: Journal of Educational Research and Innovation Technology*, *1*(2), 91–102. https://doi.org/10.34125/jerit.v1i2.7

Khubab, A. I., & Jaya, A. I. A. (2024). Implementation of Quality Education at the Darul Falah Amtsilati Islamic Boarding School. *INJIES: Journal of Islamic Education Studies*, *1*(1), 1–4. https://doi.org/10.34125/injies.v1i1.1

Kaspersky Lab. (2022). *Understanding Wireless Network Attacks*. Retrieved from https://www.kaspersky.com

Kim, J. H., Park, M., & Lee, S. (2021). A study on the security vulnerabilities of wireless networks using open-source tools. *Journal of Network Security, 18*(3), 45–53.

Kotenko, I., & Chechulin, A. (2013). A cyber attack modeling and impact assessment framework. *Proceedings of the 5th International Conference on Cyber Conflict (CyCon)*.

Laudon, K. C., & Laudon, J. P. (2020). *Management Information Systems: Managing the Digital Firm* (16th ed.). Pearson.

Ma'sum, A. H., & Purnomo, M. S. (2024). Effective Communication Strategies for Private Schools to Address the Controversy of High-Paying Education. *JERIT: Journal of Educational Research and Innovation Technology*, *1*(2), 103–111. https://doi.org/10.34125/jerit.v1i2.15

Mudijono, M., Halimahturrafiah, N., Muslikah, M., & Mutathahirin, M. (2025). Harmonization of Javanese Customs and Islamic Traditions in Clean Village. *INJIES: Journal of Islamic Education Studies*, *2*(1), 10–18. https://doi.org/10.34125/injies.v2i1.15

Mahbubi, M., & Ahmad, A. B. (2025). Redefining Education in The Millennial Age: The Role of Junior High Schools Khadijah Surabaya as A Center for Aswaja Smart Schools. *INJIES: Journal of Islamic Education Studies*, *2*(1), 19–28. https://doi.org/10.34125/injies.v2i1.14

Mahfudloh, R. I., Mardiyah, N., Mulyani, C. R., & Masuwd, M. A. (2024). Management Of Character Education in Madrasah (A Concept and Application). *INJIES:*

Journal of Islamic Education Studies, *1*(1), 35–47. https://doi.org/10.34125/injies.v1i1.5

Nugraha, R. A., & Iskandar, M. Y. (2024). Development of Video Tutorials as A Media for Learning Graphic Design in Vocational High Schools. *JERIT: Journal of Educational Research and Innovation Technology*, *1*(1), 1–11. https://doi.org/10.34125/jerit.v1i1.1

Scarfone, K., & Hoffman, P. (2008). *Guidelines for Securing Wireless Local Area Networks (WLANs)*. NIST Special Publication 800-153.

Scarfone, K., & Mell, P. (2007). *Guide to Intrusion Detection and Prevention Systems (IDPS)*. NIST Special Publication 800-94.

Sholeh, M. I., Habibulloh, M., Sokip, S., Syafi'i, A., 'Azah, N., Munif, M., & Sahri, S. (2025). Effectiveness of Blended Learning Strategy to Improving Students' Academic Performance. *JERIT: Journal of Educational Research and Innovation Technology*, *2*(1), 1–13. https://doi.org/10.34125/jerit.v2i1.17

Saputra, W., Akbar, A., & Burhanuddin, B. (2024). Modernization of Da'wah Methods in Fostering Interest Among Young Generation (Case Study QS. Al-Ahzab Verse 46). *INJIES: Journal of Islamic Education Studies*, *1*(2), 61–70. https://doi.org/10.34125/injies.v1i2.7

Septiani, D., Nugraha, M. S., Efendi, E., & Ramadhani, R. (2024). Strengthening Tuition Governance Towards Transparency and Accountability at Ummul Quro Al-Islami Modern Boarding School Bogor. *INJIES: Journal of Islamic Education Studies*, *1*(2), 83–90. https://doi.org/10.34125/injies.v1i2.10

Syafii, M. H., Rahmatullah, A. . S., Purnomo, H., & Aladaya, R. (2025). The Correlation Between Islamic Learning Environment and Children's Multiple Intelligence Development. *INJIES: Journal of Islamic Education Studies*, *2*(1), 29–38. https://doi.org/10.34125/injies.v2i1.17

Sharma, P., & Kalita, H. K. (2020). Machine learning approaches for intrusion detection: A review. *Computer Networks, 173*, 107120.

Sillaber, C., Sauerwein, C., Breu, R., & Möller, J. (2016). Data quality challenges and future research directions in threat intelligence sharing practice. *Proceedings of the 2016 ACM Workshop on Information Sharing and Collaborative Security*.

Symantec. (2020). *Wi-Fi Security and Threats: Technical Brief*. Retrieved from https://www.broadcom.com

Whitman, M. E., & Mattord, H. J. (2017). *Principles of Information Security* (6th ed.). Cengage Learning.

Yulia, N. M., Asna, U. L., Fahma, M. A., Reviana, P. A., Cholili, F. N., Halimahturrafiah, N., & Sari, D. R. (2025). Use of Game-Based Learning Media Education as An Effort to Increase Interest Elementary School Students Learning. *JERIT: Journal of Educational Research and Innovation Technology*, *2*(1), 38–45. https://doi.org/10.34125/jerit.v2i1.23

Yolanda, N. S., & Laia, N. (2024). Practicality of Mathematics Learning Media Using Applications PowToon. *JERIT: Journal of Educational Research and Innovation Technology*, *1*(1), 27–35. https://doi.org/10.34125/jerit.v1i1.4

Zafari, K. A., & Iskandar, M. Y. (2024). Interactive Multimedia Development With The Autorun Pro Enterprise Ii Application Version 6.0 In Ict Guidance In Secondary Schools. *JERIT: Journal of Educational Research and Innovation Technology*, *1*(1), 20–26. https://doi.org/10.34125/jerit.v1i1.3