MESR
منار الشرق للدراسات والأبحاث
Manar Elsharq for Studies & Research
Manar Alsharq Journal
for Education and Instructional Technology
Homepage:
http://meijournals.com/ojs/index.php/majeit/index
ISSN: 2790-6698
مجلة منار الشرق
للتربية و تكنولوجيا
التعليم

Network Security Threats and Intrusion Detection Techniques in the Era of Evolving Cyber Attacks

Noor Thamer Mahmood[1], Wisam Adnan Kareem[2], Sarmad Salih Jawad[3], Murtadha Al-Hasan[4], Ahmed Abdulrahman Abbas[5]

Computer Center, University of Babylon, Iraq[1].

Babil Education Directorate[2]

Department of Cyber Security, College of Sciences, Al-Mustaqbal University, 51001, Babylon, Iraq[3&4]

Faculty of Information Science and Technology, The National University of Malaysia, 43600 Bangi, Selangor, Malaysia[5]

استلام البحث: 28/07/2025 **مراجعة البحث:** 17/08/2025 **قبول البحث:**23/09/2025

الملخص:

مع التوسع السريع للشبكات الرقمية وتزايد تعقيد التهديدات السيبرانية، برز أمن الشبكات كمجال بالغ الأهمية في تكنولوجيا المعلومات والاتصالات. تواجه المؤسسات الحديثة مخاطر متزايدة من الهجمات السيبرانية المتطورة التي تهدد سرية الأنظمة الحيوية وسلامتها وتوافرها. أصبحت أنظمة كشف التسلل (IDS) أداة أساسية لتحديد الوصول غير المصرح به والأنشطة المشبوهة داخل الشبكات والحد منها. تُصنف هذه الأنظمة على نطاق واسع إلى أنظمة كشف التسلل القائمة على التوقيع (SIDS)، التي تعتمد على أنماط التهديد المعروفة، وأنظمة كشف التسلل القائمة على الشذوذ (AIDS)، التي تكتشف الانحرافات عن السلوك الطبيعي لتحديد الهجمات غير المعروفة. على الرغم من نقاط قوتهما، يواجه كلا النوعين قيودًا كبيرة، بما في ذلك ارتفاع معدلات الإيجابيات الكاذبة وتحديات في الكشف الفوري. تستكشف هذه الدراسة المشهد المتطور لتهديدات أمن الشبكات، وتُحلل بشكل نقدي تقنيات كشف التسلل الحالية. كما تُسلط الضوء على تكامل آليات ارتباط التنبيهات والتنبؤ التي تعزز قدرات الكشف والاستجابة المبكرة. علاوةً على ذلك، تتناول الدراسة القيود والتحديات الرئيسية في تطبيق أنظمة الكشف عن التسلل، وتحدد الاتجاهات الناشئة الهادفة إلى تحسين قابلية التوسع والذكاء والتكيف لآليات الكشف. ومن خلال تقييم الأنظمة الحالية واقتراح توجهات للأبحاث المستقبلية، يُسهم هذا العمل في تطوير استراتيجيات دفاع شبكي أكثر متانة واستباقية في عالم رقمي متزايد الترابط.

الكلمات المفتاحية: أمن الشبكات، أنظمة كشف التسلل (IDS)، التهديدات السيبرانية، كشف الشذوذ، الكشف القائم على التوقيع

Abstract

With the rapid expansion of digital networks and the increasing complexity of cyber threats, network security has emerged as a crucial field within information and communications technology (ICT). Modern organizations face growing risks from sophisticated cyber-attacks that threaten the confidentiality, integrity, and availability of critical systems. Intrusion Detection Systems (IDS) have become a foundational tool for identifying and mitigating unauthorized access and suspicious activities within networks. These systems are broadly categorized into Signature-Based Intrusion Detection Systems (SIDS), which rely on known threat patterns, and Anomaly-Based Intrusion Detection Systems (AIDS), which detect deviations from normal behavior to identify unknown attacks. Despite their strengths, both types face significant limitations, including high false-positive rates and challenges in real-time detection.

This study explores the evolving landscape of network security threats and critically analyzes existing intrusion detection techniques. It highlights the integration of alert correlation and prediction mechanisms that enhance early detection and response capabilities. Furthermore, the study addresses key limitations and challenges in IDS implementation and identifies emerging trends aimed at improving scalability, intelligence, and adaptability of detection mechanisms. By evaluating current systems and proposing directions for future research, this work contributes to the development of more robust and proactive network defense strategies in an increasingly interconnected digital world.

Keywords: Network Security, Intrusion Detection Systems (IDS), Cyber Threats, Anomaly Detection, Signature Based Detection

Introduction

With today's increasing reliance on digital networks and related systems, network security has become a major concern in many areas, particularly in information and communications technology (ICT). With the increase in cyber-attacks and their increasing sophistication, they pose a significant threat to data security and system integrity. This necessitates the need for advanced and adaptable technologies. Failure to detect these attacks early can lead to serious breaches that can severely damage system infrastructure and disrupt essential services. Intrusion detection systems (IDS) have emerged as key systems for monitoring, detecting, and responding to unauthorized and suspicious activity on networks. However, these systems face numerous limitations and challenges, including false positives and their limited ability to detect them effectively in real time. [1]

There are two categories of intrusion detection systems: signature-based intrusion detection systems (SIDS), which rely on pre-defined methods for identifying known threats, and anomaly-based intrusion detection systems (AIDS), which detect suspicious behavior to identify new and unknown attacks. Although each category of intrusion detection systems offers distinct advantages, they all face the same limitations. While intrusion detection systems are highly effective at identifying suspicious behaviors and activities that threaten the network, they struggle to counter these threats in certain situations and in various forms. [1]

In addition, the integration of intrusion detection and alerting techniques has enhanced the ability of intrusion detection systems to provide effective, timely predictions by collecting and analyzing alerts generated by isolated detections. These techniques can also correlate alerts with expected attack scenarios and provide a general overview of the network's security posture. Implementing this approach early improves early detection and response to these attacks before a full-scale attack on the network occurs. [2]

Given the increasing reliance on networks and communications systems and their critical infrastructure, there is an urgent need to develop intelligent, highly efficient, and scalable intrusion detection technologies. This study aims to examine the main threats facing networks and analyze currently available intrusion detection technologies. It also examines the current challenges facing these technologies and future trends in overcoming these challenges.

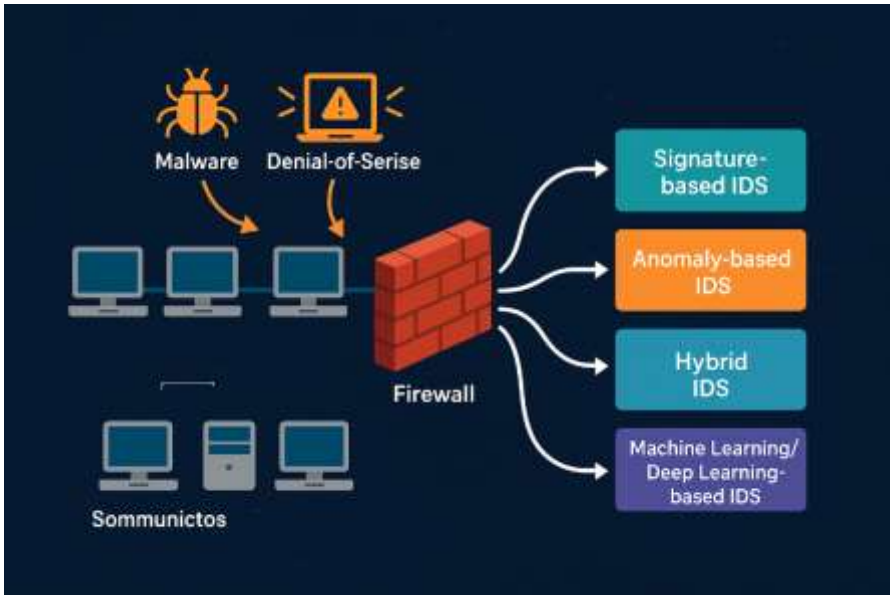

Fig (1): Cyber-attacks and intrusion detection systems

Problem Statement

With the growth of networked systems, communications, and Internet-connected devices, network security has become increasingly vulnerable to cyberattacks and threats. Traditional security measures and technologies, such as firewalls and full access control, are often ineffective in detecting and countering these attacks. Therefore, intrusion detection systems (IDS) have become critical tools for identifying suspicious attacks and unauthorized activity within the network.

However, these systems face several limitations that limit their effectiveness. Signature-based systems primarily operate on pre-defined methods and patterns of known attacks. Anomaly-based systems, while capable of detecting new and unknown attacks, generate false alarms at a high rate due to the difficulty of accurately controlling network behavior. In addition, intrusions proceed through obvious steps, such as malicious connection formation and excessive buffer consumption. These steps can be integrated into normal traffic patterns, but distinguishing between suspicious and normal traffic remains a major technical challenge. Evaluation metrics for intrusion detection systems, such as accuracy, timeliness, comprehensiveness, fault tolerance, and scalability, still pose challenges in diverse environments [3]. Therefore, this research seeks to examine the strengths and weaknesses of current intrusion detection systems and identify approaches that address modern network security challenges.

Research objectives

The primary objective of this study is to identify attacks facing network security and analyze intrusion detection systems that counter these attacks. The study aims to:

1. Study the most prominent attacks and threats that attack network environments and how they affect data security and integrity.
2. Analyze and classify different types of intrusion detection systems, studying their structure and nature of operation.
3. Identify the advantages and disadvantages of traditional intrusion detection systems and common detection methods.
4. Study the challenges facing traditional intrusion detection systems, such as false positives, their adaptability, scalability, and development.
5. Suggest potential improvements to these systems to improve the accuracy, efficiency, effectiveness, and intelligence of intrusion detection systems to mitigate potential attacks and threats.

Significance of the Research

The importance of this research focuses on protecting digital networks and communications from advanced cyber-attacks and intrusions by studying various intrusion detection techniques and systems. The research supports the development of more effective, accurate, and intelligent technologies, focusing on techniques that detect and counter these attacks in various environments. Additionally, it focuses on identifying the challenges facing these systems and developing radical solutions to improve the effectiveness of all intrusion detection systems. This study contributes to encouraging the

development of intrusion detection systems with high capabilities to detect known and emerging cyber-attacks.

Related research /Background of the protocol

The rapid evolution of network environments, the complexity of their infrastructure, and the rapid spread of the Internet of Things have led to a relatively high rate of cyberattacks. This has necessitated the development of advanced and highly efficient intrusion detection systems (IDSs) to counter these attacks and adapt to the specific network environment in which the attack occurs. Although traditional intrusion detection systems, such as signature-based systems, are highly effective in countering known and previously identified attacks, they struggle to identify new cyberattacks. Similarly, anomaly-based systems, despite their flexibility and ability to detect new attacks, produce relatively high false positive rates and are computationally expensive. To enhance the adaptability and scalability of these systems in distributed network environments, some agent-based IDS architectures have been proposed. Lee et al. developed a multi-agent defense system that combines data mining and real-time analysis. The system has proven effective in detecting large-scale attacks and unauthorized activities by autonomous agents, but it has faced significant challenges in deployment and generalization [3]. For his part, Baker et al. emphasized the importance of simulating realistic traffic in testing intrusion detection systems (IDSs). He criticized the incorrect use of metrics such as curves in static signature-based systems and emphasized the need for standardized testing methods [4].

Holdbrook et al. (2024) conducted a comprehensive comparative analysis of supervised machine learning classifiers including Naive Bayes, Decision Trees, and Support Vector Machines using the KDDCup99 dataset. Their results emphasized the significant role that appropriate feature selection plays in improving detection accuracy, especially in network intrusion detection scenarios . [5].

Medeiros et al. presented a comprehensive and integrated taxonomy of network anomaly detection techniques, focusing on integrating real-time analysis, feature selection, and hybrid detection methods [6]. Additionally, Arnob et al. structured network attacks and their detection systems into attacker/defender configurations and discussed the scalability of real-time intrusion detection tools [7].

Alnajimet al. proposed hybrid data mining approaches such as K-means and naive Bayes models to enhance detection accuracy and efficiency and reduce false positive rates [8]. Krishna and Selvapriya study focused on the limitations of traditional network security, such as firewalls, and urged the development of adaptive intrusion detection systems based on neural networks and swarm intelligence [9].

Vaishalini et al. mapped the development of intrusion detection systems, moving from classical learning to deep learning (DL), focusing on ensemble models and datasets such as NSL-KDD and UNSW-NB15 for testing and evaluation [10]. Hewapathirana proposed a two-stage intrusion detection framework using the CSE-CIC-IDS2018 dataset, leveraging stacked auto encoders and Apache Spark-based classifiers. Her study analyzed different attack types including DoS, FTP-Brute Force, and Infiltration and highlighted the trade-offs between detection accuracy and computational efficiency, suggesting future directions toward adaptive hybrid IDS models. [11]. Ali et al. conducted a comprehensive survey on machine learning (ML) and deep learning (DL) techniques used in intrusion detection systems (IDSs). The study explored various ML and DL approaches, including multilayer perceptrons (MLPs), and discussed their applicability in distributed and real-time environments such as the Internet of Things (IoT). The authors emphasized performance metrics, dataset challenges, and deployment considerations in modern IDS implementations [12]. Sharma and Chen systematically examined adversarial attacks targeting ML-based network intrusion detection systems. Their analysis focused on black-box and white-box attacks such as Projected Gradient Descent (PGD),

HopSkipJump, and Zeroth-Order Optimization (ZOO), revealing the vulnerabilities of commonly used classifiers like MLP and logistic regression to adversarial manipulation. The study underscored the urgent need for developing more robust IDS models in adversarial environments [13]. Ashraf et al. presented an in-depth review of machine learning and deep learning-based intrusion detection systems tailored for IoT security. The study highlighted techniques such as support vector machines (SVMs), multilayer perceptrons (MLPs), and ant colony optimization, with a particular focus on issues related to data imbalance, high dimensionality, and computational efficiency. The paper also discussed future directions for building scalable and intelligent IDS frameworks [14]. In addition, Dina and Manivannan discussed the transformation of intrusion detection systems into AI-based systems capable of handling known and unknown threats using supervised and unsupervised models [15].

Hidori et al. addressed the security vulnerabilities in non-contiguous data networks (NDNs). They focused on the security of these networks, their vulnerability to cache-related attacks, and the urgent need for AI-based intrusion detection systems specifically designed for these types of networks [16]. Dania et al. demonstrated the effectiveness of classical machine learning and deep learning models on the UNSW-NB15 dataset, particularly models with a CNN architecture that achieved high detection accuracy against various attacks [17].

Shiravani et al. presented a hybrid model that combines fuzzy logic, correlation-based feature selection, and genetic algorithms, achieving a high accuracy of 99.9% in intrusion detection [18]. De Alwis et al. explored the vulnerabilities of 5G network segmentation, emphasizing the need to develop AI-based, slice-specific detection systems to address high-performance, dynamic environments [19]. Al-Khawlani et al. highlighted the severe and significant gap in research on IoT attacks and IoT intrusion detection systems and called for lightweight and adaptable solutions [20]. Rahman et al. reviewed hybrid machine learning and deep learning solutions for IoT intrusion detection systems, introducing models such as RFE, SMOTE, XGBoost, and CNN-BiLSTM to address imbalanced data and resource constraints [21]. All these studies provide strong evidence that hybrid machine learning and deep learning models and methods have high intrusion detection capabilities and are suitable for adapting to the unique constraints and modern threats, especially IoT attacks. These studies form the basis for developing next-generation intrusion detection system protocols that are characterized by artificial intelligence, flexibility, and scalability in the face of attacks.

Methodology / Design Formula

This study adopts a qualitative survey-based research methodology. It aims to collect and analyze the available literature on cyber-attacks on network security and intrusion detection techniques to counter these attacks, and to conduct a comprehensive evaluation of these techniques. The methodology is divided into several stages, including a thorough and balanced review of contemporary and classical research in the field of network security. These stages are as follows:

1. Literature Collection and Review

A comprehensive systematic literature review framework was adopted to identify and collect relevant research papers and studies from major and reliable academic platforms such as IEEE Xplore, Springer, ScienceDirect, and Elsevier. The focus was on peer-reviewed research studies and scientific articles from 2004 to 2025, covering network attack methods and traditional and hybrid intrusion detection approaches that incorporate some smart models based on artificial intelligence, machine learning, and deep learning.

2. Comparative Analysis

The main intrusion detection techniques were analyzed into main categories in terms of their

architecture, learning algorithms, and deployment environments, and compared based on several evaluation criteria:

- Detection accuracy
- Hit rates
- Computational complexity
- Their ability to adapt to zero-day attacks
- Their scalability and suitability for the Internet of Things and distributed networks

The comparison of these techniques is based on datasets used in these techniques, such as KDD99, NSL-KDD, UNSW-NB15, and CICIDS2017. These datasets are widely used to evaluate intrusion detection systems in academic studies.

Technique	Accuracy	Adaptability	False Positives	Complexity	Use Case Suitability
Signature-Based IDS	High	Low	Low	Low	Known threats, enterprise
Anomaly-Based IDS	Medium	High	High	Medium	Dynamic networks
Hybrid IDS	High	High	Medium	High	Critical systems
ML/DL-Based IDS	Very High	Very High	Medium-Low	High	IoT, Cloud, 5G, Smart cities

Table (1): Comparison between intrusion detection systems

3. Classification of Technologies

Studies and detection techniques were classified according to a specific pattern (from oldest to newest):

- Signature-based intrusion detection techniques (SIDS)
- Anomaly-based intrusion detection techniques (AIDS)
- Hybrid intrusion detection techniques
- Machine learning and deep learning-based intrusion detection techniques

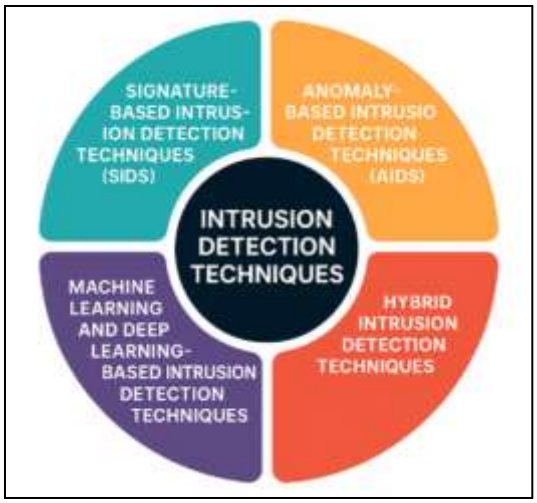

Fig (2): Intrusion detection systems categories

4. Critical and Objective Analysis

Critical and objective analysis of the selected studies was conducted to analyze and compare the different results to identify:

- Limitations and challenges facing intrusion detection systems
- Future trends and future developments in AI-integrated intrusion detection system architectures
- Gaps in research related to real-time attack handling and rare attack detection

5. Synthesis and Research Gaps

By collecting and studying methodologies and comparing them across multiple groups of intrusion detection system architectures. This study identifies commonalities, ongoing challenges, and gaps in the field, including:

- The urgent need for highly adaptive systems for network anomaly detection
- The ongoing challenges in reducing false positive rates
- The lack of a unified roadmap for comparison between studies
- The call for hybrid models that combine interpretability and high accuracy.

Conclusion

This study provides a comprehensive overview of the reality of network security threats and cyberattacks, as well as intrusion detection systems and their rapid developments, through a detailed study of various intrusion detection systems, such as signature-based, anomaly-based, hybrid models, and systems based on machine learning and deep learning. It was demonstrated that traditional systems, despite their importance, are largely insufficient to address the advanced and complex challenges, and there is no single effective solution to address these cyberattacks. Furthermore, these systems still face numerous challenges that limit their effectiveness. Signature-based detection systems

are effective in detecting known and specific attacks, but they struggle to counter new and unknown attacks. Anomaly-based systems, on the other hand, have significant capabilities in detecting new and unknown attacks, but they struggle to handle false positives and false alarms. Hybrid models have subsequently demonstrated clear and effective progress in balancing accuracy and detection efficiency by combining the strengths of several different technologies. Machine learning- and deep learning-powered systems have opened new horizons for early and intelligent detection of cyberattacks in various complex environments, such as the Internet of Things, distributed networks, and 5G networks. These systems have become more adaptive, intelligent, and capable of evolving as attacks evolve. However, many challenging issues remain that prevent these systems from performing as intended. These challenges include limitations on available datasets, scalability issues in distributed environments, especially in Internet of Things networks, problems with detecting zero-day attacks, and the difficulty of deploying lightweight, scalable intrusion detection systems across distributed systems.

Results

The results of this study were derived from a comprehensive analysis and study of the literature and available studies on network attacks and network intrusion detection techniques. These results are summarized as follows:

1. **Signature-based intrusion detection systems (SIDS)**
   - Advantages: Fast detection, low computational costs, and effective against known and identified cyber-attacks.
   - Limitations: Incapable of detecting new and unknown attacks, including zero-day attacks, and require continuous signature updates.
2. **Anomaly-based intrusion detection systems (AIDS)**
   - Advantages: Capable of detecting new and unknown attacks based on normal behavior.
   - Limitations: High false positive rates and sensitive to the quality of test data.
3. **Hybrid intrusion detection systems**
   - Advantages: Combine the accuracy of SIDS with the flexibility of AIDS, resulting in high detection capacity.
   - Limitations: High complexity and high resource consumption.
4. **Machine learning and deep learning-based intrusion detection systems.**
   - Advantages: High accuracy, scalability, adaptability to advanced attacks, and efficient performance in traffic patterns.
   - Limitations: Requires large data sets, is difficult to interpret, and is vulnerable to adversarial attacks.

Recommendations

1. Develop intrusion detection systems that are adaptable to various dynamic environments and user behavior patterns in real time.

2. Combine traditional and AI-powered systems to develop more robust and interpretable systems that reduce false positive rates.

3. Provide large real-world datasets, including threat patterns from the Internet of Things, distributed networks, and 5G networks.

4. Build adaptive, self-learning intrusion detection systems capable of continuous learning, both unsupervised and semi-supervised.

By addressing these research gaps, future intrusion detection system solutions can evolve into effective, intelligent, adaptive, and scalable systems capable of securing networks against known and emerging cyberattacks.

Furthermore, this study proposes the design of a next-generation adaptive intrusion detection system (A-IDS), powered by artificial intelligence (AI). This system integrates real-time data analysis, continuous learning through federated machine learning, and rapid automated response mechanisms. This approach can significantly reduce false positives and improve scalability in pervasive environments such as the Internet of Things (IoT) and 5G networks, enabling the proactive detection of zero-day attacks.

References

[1] Makris, I., et al. (2025). A comprehensive survey of Federated Intrusion Detection Systems: Techniques, challenges and solutions. Computer Science Review, 56, 100717. https://doi.org/10.1016/j.cosrev.2024.100717 [Q1]

[2] Albasheer, H., Md Siraj, M., Mubarakali, A., et al. (2022). Cyber-attack prediction based on network intrusion detection systems for alert correlation techniques: A survey. Sensors, 22(4), 1494. https://doi.org/10.3390/s22041494

[3] Diana, L., Dini, P., & Paolini, D. (2025). Overview on Intrusion Detection Systems for Computers Networking Security. Computers, 14(3), 87. https://doi.org/10.3390/computers14030087

[4] Shan, J., Ma, H., & Li, J. (2024). Research on network attack sample generation and defence techniques based on generative adversarial networks. Applied Mathematics and Nonlinear Sciences, 9(1), 1–20. https://www.sciendo.com

[5] Holdbrook, O. B., Adu-Manu, K. S., Owusu, E., & Essien, B. (2024). A Comprehensive Study on Machine Learning Techniques for Intrusion Detection. Electronics, 13(4440), 1–28. https://doi.org/10.3390/electronics13144440

[6] Medeiros, F. N., Lima, G. B., & de Carvalho, A. C. P. L. F. (2023). A Survey on Network Anomaly Detection Using Machine Learning. Sensors, 23(1352), 1–28. https://doi.org/10.3390/s23031352

[7] Arnob, A. K. B., Chowdhury, R. R., Chaiti, N. A., Saha, S., & Roy, A. (2025). A comprehensive systematic review of intrusion detection systems: Emerging techniques, challenges, and future research directions. Journal of Edge Computing, 4(1), 73–104. https://doi.org/10.55056/jec.885

[8] Alnajim, A. N., Hameed, A. I., & Mahdi, N. A. (2023). A Comprehensive Survey of Cybersecurity Threats, Attacks, and Effective Countermeasures in Industrial Internet of Things. Technologies, 11(161), 1–15. https://doi.org/10.3390/technologies11020161

[9] Krishna, R. H., & Selvapriya, B. (2024). Comprehensive Review of Intrusion Detection Systems in Cloud Computing. International Journal of Intelligent Systems and Applications in Engineering, 12(3), 724–731.

[10] Vaishalini, V. G. S., Ramathilagam, A., Palanikumar, R., Raghavan, P., Gopikannan, P., & Manikandan, K. (2024). Comprehensive Survey of Deep Learning-Based Intrusion Detection and Prevention Systems for Secure Communication in the Internet of Things. International Journal of Intelligent Systems and Applications in Engineering, 12(3), 1822–1828.

[11] Hewapathirana, I. U. (2025). A comparative study of two-stage intrusion detection using modern machine learning approaches on the CSE-CIC-IDS2018 dataset. Knowledge, 5(1), 6. https://doi.org/10.3390/knowledge5010006

[12] Ali, H. A., Charfeddine, M., Ammar, B., Hamed, B. B., Albalwy, F., Alqaraawi, A., & Hussain, A. (2024). Unveiling machine learning strategies and considerations in intrusion detection systems: A comprehensive survey. Frontiers in Computer Science, 6, 1387354. https://doi.org/10.3389/fcomp.2024.1387354

[13] Sharma, S., & Chen, Z. (2024). A systematic study of adversarial attacks against network intrusion detection systems. Electronics, 13(24), 5030. https://doi.org/10.3390/electronics13245030

[14] Ashraf, J., Moustafa, N., Khurshid, H., Debie, E., Haider, W., & Wahab, A. (2020). A review of intrusion detection systems using machine and deep learning in Internet of Things: Challenges, solutions and future directions. Electronics, 9(7), 1177. https://doi.org/10.3390/electronics9071177

[15] Deepa, V., & Radha, N. (2021). A survey on network intrusion system attacks classification using machine learning techniques. IOP Conference Series: Materials Science and Engineering, 1022(1), 012036. https://doi.org/10.1088/1757-899X/1022/1/012036 [Q3]

[16] Dina, A. S., & Manivannan, D. (2021). Intrusion detection based on machine learning techniques in computer networks. Internet of Things, 16, 100462. https://doi.org/10.1016/j.iot.2021.100462 [Q1]

[17] Hidouri, A., Hajlaoui, N., Touati, H., Hadded, M., & Muhlethaler, P. (2022). A survey on security attacks and intrusion detection mechanisms in Named Data Networking. Computers, 11(12), 186. https://doi.org/10.3390/computers11120186 [Q2]

[18] Dhanya, K. A., Vajipayajula, S., Srinivasan, K., Tibrewal, A., Kumar, T. S., & Kumar, T. G. (2023). Detection of network attacks using machine learning and deep learning models.

Procedia Computer Science, 218, 57–66. https://doi.org/10.1016/j.procs.2022.12.401 [Q3]

[19] Shiravani, A., Sadreddini, M. H., & Nahook, H. N. (2023). Network intrusion detection using data dimensions reduction techniques. Journal of Big Data, 10(27). https://doi.org/10.1186/s40537-023-00697-5 [Q1]

[20] De Alwis, C., Porambage, P., Dev, K., Gadekallu, T. R., & Liyanage, M. (2024). A Survey on Network Slicing Security: Attacks, Challenges, Solutions and Research Directions. IEEE Communications Surveys & Tutorials, 26(1), 534–566. https://doi.org/10.1109/COMST.2023.3312349 [Q1]

[21] Alkhawlani, Z., Ibrahimi, K., & Boutabia, M. (2024). Intrusion detection systems for the Internet of Things network: Survey on rare attacks. In S. A. R. Zaidi, K. Ibrahimi, M. ElKamili, A. Kobbane, & N. Aslam (Eds.), Proceedings of the 11th International Conference on Wireless Networks and Mobile Communications (WINCOM 2024) (pp. 498–503). IEEE. https://doi.org/10.1109/WINCOM62286.2024.10655360

[22] Rahman, M. M., Shakil, S. A., & Mustakim, M. R. (2025). A survey on intrusion detection system in IoT networks. Cyber Security and Applications, 3, 100082. https://doi.org/10.1016/j.csa.2024.100082 [Q2]