



JOURNAL OF SCIENCE, TECHNOLOGY AND EDUCATION (JSTE)



**A PUBLICATION OF THE
DEPARTMENT OF SCIENCE,
TECHNOLOGY AND MATHEMATICS
EDUCATION (STME),
NASARAWA STATE UNIVERSITY, KEFFI, NIGERIA**



VOLUME 10

ISSN: 2651-5539

EVALUATION OF THE ROLES OF ARTIFICIAL INTELLIGENCE IN ENHANCING CYBERSECURITY THREAT DETECTION AND RESPONSE IN JIGAWA STATE, NIGERIA

¹Muazu B. S., ²Aliyu M. and ³Yahaya A. A

^{1,2}Department of Computer Science Education, Jigawa State College of Education and Legal Studies, Ringim

³North-West University, Kano, Kano State, Nigeria

Corresponding author: bmuazu@jcoels.edu.ng

Citation: Muazu B. S., Aliyu M. & Yahaya A. A. (2026). Influence of teachers' content knowledge and attitude towards teaching on Students' Interest and achievement in genetics in Nasarawa West Senatorial District of Nasarawa State. *Journal of Science, Technology, and Education (JSTE)*; www.nsukjste.com/. 10(37), 511-523.

Abstract

Artificial Intelligence (AI) has become an important technology for enhancing cybersecurity threat detection and response as cyber threats continue to increase in sophistication and frequency. This study evaluated the role of AI in improving cybersecurity threat detection and response in Jigawa State, Nigeria. Specifically, the study examined AI's contribution to cybersecurity operations and evaluated the effectiveness of Random Forest, Long Short-Term Memory (LSTM), and Autoencoder models for detecting cyber threats. A descriptive survey research design was adopted. Data were collected from 100 respondents comprising cybersecurity professionals, information technology personnel, software developers, academic staff, and students with knowledge of Artificial Intelligence and cybersecurity using a structured questionnaire with a reliability index of 0.84. Two research questions were asked. The data was collected and analysed using means and standard deviations. The findings revealed that respondents agreed that AI significantly

improves threat-detection accuracy, enables real-time monitoring, reduces incident-response time, detects previously unknown threats, and supports automated incident response. The findings also showed that all three AI models were effective in detecting cyber threats, with LSTM having the highest mean score, followed by Random Forest and Autoencoder. The study concludes that AI significantly enhances cybersecurity threat detection and response when integrated with conventional security mechanisms and supported by skilled cybersecurity professionals. The study recommends, among others, that increased adoption of AI-based cybersecurity solutions, investment in advanced AI models, continuous professional training, and the development of ethical guidelines to support responsible AI deployment in cybersecurity.

Keywords: Evaluation, Artificial Intelligence, Cybersecurity, Intrusion Detection Systems, Threat Detection, Threat Response, Anomaly Detection.

Introduction

The rapid growth of digital technologies has transformed nearly every aspect of modern life. Sectors such as healthcare, finance, transportation, education, and industrial control systems now depend heavily on interconnected digital infrastructures to support daily activities and services. While these developments have improved efficiency, communication, and innovation, they have also created new cybersecurity challenges. As organizations become increasingly dependent on digital systems and data-driven operations, cyber threats continue to grow in both scale and complexity, making cybersecurity a critical concern for governments, institutions, and businesses around the world.

Cyberattacks have changed considerably over the years. Earlier attacks were often easier to detect and generally less sophisticated, whereas modern threats are more adaptive, coordinated, and difficult to identify. Many attacks are driven by financial or political motives and commonly involve ransomware, malware, advanced persistent threats (APTs), and zero-day exploits. Attackers frequently attempt to remain undetected for extended periods while bypassing traditional security controls. Studies indicate that the expansion of digital infrastructures has been accompanied by a steady increase in sophisticated cyber threats (Hozouri et al., 2025).

Conventional cybersecurity systems rely mainly on rule-based and signature-based detection techniques. These methods compare network activity against predefined attack signatures or known malicious behaviours. Although they remain effective against previously identified threats, they are often less successful in detecting new or rapidly evolving attacks. Signature-based systems may fail to identify zero-day vulnerabilities, while rigid rule-based methods can struggle to adapt to changing network environments. Consequently, many traditional security systems operate reactively rather than proactively, responding only after an attack has occurred (Mohamed, 2023).

The limitations of traditional cybersecurity approaches have encouraged greater adoption of Artificial Intelligence (AI) in security operations. AI technologies, particularly machine learning (ML) and deep learning (DL), can analyze large volumes of data, identify complex relationships, and adapt to changing conditions without relying entirely on predefined instructions. These capabilities make AI valuable for detecting unusual behaviour and identifying previously unseen threats in complex network environments. One of the most significant advantages of AI-driven cybersecurity systems is their ability to operate in real time. Unlike conventional approaches that depend heavily on manual updates and static rules, AI models can

continuously monitor network activity and react quickly to suspicious behaviour. This capability is especially important in situations where delayed detection can result in financial losses, operational disruption, or data compromise.

Beyond threat detection, AI is increasingly being used in practical cybersecurity environments. Organizations now apply AI-driven technologies in cloud security monitoring, financial fraud detection, Security Operations Center (SOC) automation, and threat intelligence platforms. These developments demonstrate that AI is no longer confined to research environments but is becoming an important part of everyday cybersecurity practice, particularly in settings that generate large volumes of security data and face constantly evolving threats.

Despite the progress made in AI-based cybersecurity research, several challenges remain. Much of the existing literature focuses on improving detection accuracy using benchmark datasets, while issues such as real-world deployment, model generalization, explainability, ethical considerations, operational constraints, and human oversight often receive less attention. As a result, models that perform well under controlled testing conditions may not always achieve the same level of success in dynamic operational environments.

This study examines the role of Artificial Intelligence in enhancing cybersecurity threat detection and response. Specifically, it evaluates the effectiveness of machine learning and deep learning techniques in identifying cyber threats, compares the strengths and limitations of selected AI approaches, and explores the ethical, operational, and practical challenges associated with their deployment. By looking beyond technical performance alone, the study aims to provide a broader understanding of how AI can be integrated effectively into modern cybersecurity operations. The findings contribute to ongoing discussions on the responsible and practical use of AI in addressing contemporary cybersecurity challenges.

Statement of the Problem

The growing reliance on digital technologies across organizations and critical sectors has increased exposure to cyber threats. Attacks such as ransomware, malware, advanced persistent threats, and zero-day exploits continue to evolve in complexity, making them more difficult to detect and manage. Traditional cybersecurity approaches, which rely largely on predefined rules and known attack signatures, often struggle to respond effectively to emerging and previously unseen threats.

Recent developments in machine learning and deep learning have introduced new opportunities for improving cybersecurity operations. While existing studies frequently report high detection accuracy for AI-based systems, much of the research focuses on performance within controlled environments and benchmark datasets. Less attention has been given to practical implementation issues, including model interpretability, operational challenges, ethical concerns, and the role of human expertise in security decision-making. Consequently, there is a need for a broader examination of how intelligent technologies can support cybersecurity threat detection and response in real-world environments. This study addresses that need by examining the capabilities, limitations, and practical relevance of selected AI techniques in modern cybersecurity operations.

Research Objectives

The main objective of this study is to investigate the roles of Artificial Intelligence in enhancing cybersecurity threat detection and response. The specific objectives are to:

1. Evaluate the contribution of AI to cybersecurity threat detection and response;
2. Evaluate the effectiveness of Random Forest, Long Short-Term Memory

(LSTM), and Auto encoder models in detecting cyber threats;

Research Questions

The study had the following research questions:

1. What are the contributions of AI in cybersecurity threat detection and response?
2. What is the effectiveness of Random Forest, LSTM, and Auto encoder models in detecting cyber threats?

Literature Review

Artificial Intelligence (AI) has become one of the most important technologies shaping modern cybersecurity. As cyber threats continue to grow in complexity, speed, and frequency, traditional security systems that rely mainly on fixed rules and signature-based detection are no longer sufficient. Modern attacks often evolve rapidly and can bypass conventional defenses, making it difficult for organizations to respond effectively. AI offers a more adaptive solution because it enables systems to learn from data, identify hidden patterns, and detect suspicious behavior in real time. For this reason, AI is now widely recognized as a major component of modern cybersecurity systems.

Several studies show that AI techniques, particularly machine learning, can significantly improve intrusion detection systems (IDS) (Hozouri et al., 2025). It is also explained that AI-driven models outperform many traditional approaches, especially in detecting both familiar and previously unknown cyber threats. Likewise, Mohamed (2023) notes that AI systems can process very large volumes of network traffic quickly, allowing security teams to identify suspicious activity faster and respond more efficiently. These findings demonstrate the growing importance of intelligent systems in protecting digital infrastructures.

The development of deep learning has further strengthened cybersecurity capabilities. Deep learning techniques are designed to extract complex patterns from large datasets, making them highly suitable for analyzing network traffic and detecting cyberattacks. Models such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) have shown strong performance in identifying hidden attack behaviors. Despite these advantages, researchers also caution against overestimating the effectiveness of AI in practical cybersecurity environments. One major issue is the difference between laboratory performance and real-world deployment (Ring et al., 2019). It is further noted that many AI models are tested using benchmark datasets that do not fully reflect

real network conditions (Verkerken et al., 2022). Problems such as dataset bias and limited data diversity can therefore produce overly optimistic performance results. As a result, systems that appear highly accurate during testing may struggle when deployed in real operational settings.

A further concern is data quality. AI systems rely heavily on well-structured and representative datasets. When datasets are incomplete, poorly labeled, or imbalanced, the performance of AI models can decline significantly (Sarhan et al., 2022). It is emphasized that the success of AI-based intrusion detection systems depends greatly on the quality and realism of the training data. This highlights the need for more comprehensive datasets that better capture real-world cybersecurity challenges. Taken together, existing research suggests that AI has strong potential to transform cybersecurity, but its long-term effectiveness will depend on addressing issues related to data quality, generalization, and practical implementation.

Although AI offers major benefits in cybersecurity, several challenges continue to limit its effectiveness. One important issue is bias and data limitation. AI systems depend strongly on training data, and when datasets are biased or incomplete, models may produce inaccurate or unfair results (Mehrabi et al.,

2021). It is discussed that bias in machine learning can negatively affect both system fairness and overall performance.

A further challenge is adversarial attacks, where attackers intentionally manipulate input data to deceive AI models (Biggio & Roli, 2018). It is demonstrated that adversarial machine learning poses a serious threat to AI-based cybersecurity systems, while Papernot et al. (2017) show that even advanced deep learning models can be misled by carefully crafted inputs.

The lack of explainability also remains a major obstacle. In many cases, cybersecurity professionals cannot clearly understand how AI systems reach their decisions, making it difficult to trust their outputs. Although explainable AI has been proposed as a possible solution, its practical implementation in cybersecurity is still developing (Arrieta et al., 2020).

Ethical and regulatory concerns also continue to grow. It is emphasised that ethical frameworks are essential for guiding the responsible use of AI (Floridi et al., 2018), while Jobin et al. (2019) stress the need for global standards that ensure fairness, accountability, and transparency. Beyond these concerns, operational challenges such as high computational costs, limited expertise, and the need for significant financial investment also make AI adoption difficult for many organisations, especially smaller

institutions. It is further noted that overreliance on automation without proper human oversight may introduce additional risks (Sarker, 2022).

Despite significant progress in AI-based cybersecurity research, important gaps still exist. Much of the current literature focuses mainly on improving detection accuracy using benchmark datasets that do not fully represent real-world conditions. It is explained that many intrusion detection systems fail to generalise effectively in operational environments (Verkerken et al., 2022), while Ferrag et al. (2022) called for more realistic evaluation methods. Furthermore, ethical issues such as transparency, fairness, and accountability are often overlooked in technical research.

This study addresses these limitations by adopting a broader perspective that considers not only technical performance but also ethical, operational, and practical dimensions. Through this approach, the study aimed to provide a more balanced understanding of how AI could be effectively applied in modern cybersecurity,

Methodology

This study employed a descriptive survey research design to investigate the use of Artificial Intelligence (AI) to enhance cybersecurity threat detection and response. The survey design was considered appropriate because it enabled the researcher to obtain

first-hand information from respondents with knowledge and experience in information technology and cybersecurity. The design also provided an opportunity to examine respondents' perceptions and experiences regarding the effectiveness, challenges, and adoption of AI-based cybersecurity systems. The study was conducted among individuals with knowledge of information technology and cybersecurity. The respondents included cybersecurity professionals, IT personnel, network administrators, software developers, academic staff, and students with relevant knowledge of cybersecurity and Artificial Intelligence.

The study population comprised cybersecurity professionals, IT personnel, software developers, academic staff, and students with knowledge of Artificial Intelligence and cybersecurity. This population was selected because of its familiarity with cybersecurity threats, AI applications, and contemporary digital security practices. A sample of 100 respondents was selected from the target population using purposive sampling. Purposive sampling was adopted because the study required respondents with adequate knowledge and experience in Artificial Intelligence and cybersecurity. Only properly completed questionnaires were included in the analysis.

The instrument used for data collection was a structured questionnaire developed by the researcher, based on the study's objectives and relevant literature on Artificial Intelligence and cybersecurity. The questionnaire consisted of two sections. Section A elicited demographic information from respondents, including gender, age, educational qualification, occupation, and years of experience in information technology or cybersecurity. Section B contained items designed to obtain information on the application of Artificial Intelligence in cybersecurity threat detection, the effectiveness of AI techniques in detecting cyber threats, the challenges associated with AI implementation, and strategies for improving AI-based cybersecurity systems.

To ensure that the questionnaire measured the intended variables, the instrument underwent face and content validation by experts in cybersecurity, information technology, and educational research. Their observations and recommendations were incorporated into the final version of the questionnaire before administration. The responses obtained from the pilot study were analyzed using Cronbach's Alpha, yielding a reliability coefficient of 0.84. This value indicated that the questionnaire possessed satisfactory internal consistency and was suitable for data collection.

The researcher administered the questionnaire to the selected respondents using both printed and electronic formats. Before administering the instrument, respondents were informed of the purpose of the study and assured that the information provided would be kept confidential and used solely for academic purposes. Completed questionnaires were collected, screened for completeness, and coded for analysis. Questionnaires with incomplete or inconsistent responses were

excluded from the final analysis to ensure data accuracy and quality.

Data collected from respondents were coded and analyzed using descriptive statistics. Frequencies, percentages, mean scores, and standard deviations were used to summarize respondents' demographic characteristics and answer the research questions. The findings are presented using tables, charts, and graphical illustrations to facilitate interpretation and discussion.

Results

Research Question One

What are the contribution of AI in cybersecurity threat detection and responses?

Table 1: Respondents' Opinion on the Contribution of AI to Cybersecurity Threat Detection and Response (N = 100)

Items	Strongly Agree (SA)	Agree (A)	Undecided (U)	Disagree (D)	Strongly Disagree (SD)	Mean	Decision
AI improves the accuracy of threat detection	52	35	6	4	3	4.29	Accepted
AI enables real-time monitoring of cyber threats	48	38	7	5	2	4.25	Accepted
AI reduces the response time to cyber incidents	45	39	8	5	3	4.18	Accepted
AI detects previously unknown cyber threats	46	37	9	3	3	4.18	Accepted
AI supports automated incident response	43	40	8	6	3	4.14	Accepted
Grand Mean	—	—	—	—	—	4.21	Accepted

Table 1 indicates that respondents generally agreed that Artificial Intelligence makes significant contributions to cybersecurity threat detection and response. The grand mean of **4.21** exceeds the benchmark mean of **3.00**, indicating overall agreement. Respondents agreed, in particular, that AI improves threat-

detection accuracy, enables continuous monitoring, reduces response time, detects emerging cyber threats, and supports automated security operations. Therefore, Artificial Intelligence contributes positively to cybersecurity threat detection and response.

Research Question Two

What is the effectiveness of Random Forest, LSTM, and Autoencoder models in detecting cyber threats?

Table 2: Effectiveness of AI Models in Cyber Threat Detection (N = 100)

AI Model	Very Effective	Effective	Undecided	Ineffective	Very Ineffective	Mean	Decision
Random Forest	42	40	9	6	3	4.12	Effective
LSTM	56	31	6	4	3	4.33	Highly Effective
Autoencoder	38	39	12	7	4	4.00	Effective

Table 2 reveals that all three Artificial Intelligence models were considered effective in detecting cybersecurity threats. Among them, the LSTM model recorded the highest mean score (4.33), indicating that respondents perceived it as the most effective technique because of its ability to learn sequential attack

patterns and identify sophisticated threats. Random Forest ranked second with a mean score of 4.12, while Autoencoder ranked third with a mean score of 4.00. Overall, the findings suggest that LSTM is the most effective among the evaluated AI models.

Discussion of Findings

The findings of this study revealed that Artificial Intelligence (AI) plays a significant role in improving cybersecurity threat

detection and response. Responses obtained from the participants showed strong agreement that AI enhances the accuracy of threat detection, supports continuous monitoring of network activities, reduces the

time required to respond to cyber incidents, identifies previously unknown attacks, and facilitates automated incident response. The high grand mean recorded for the first research question indicates that respondents generally perceived AI as an important tool for strengthening cybersecurity operations.

This finding agrees with the work of Sarker et al. (2021), who reported that machine learning techniques improve the capability of intrusion detection systems by analysing large volumes of network traffic and identifying malicious activities more accurately than traditional rule-based systems. The result is also consistent with (Mohamed, 2023), who observed that AI enables security systems to detect abnormal network behaviour in real time, thereby allowing organizations to respond to threats more quickly. The implication is that AI offers a proactive approach to cybersecurity by identifying suspicious activity before it escalates into major security breaches.

The study further established that AI improves operational efficiency in cybersecurity. Automated threat detection and response reduce the workload of cybersecurity personnel, minimize human errors, and enable organizations to respond rapidly to emerging threats. This supports the assertion of (Hozouri et al., 2025) that intelligent cybersecurity systems are capable of adapting

to evolving attack patterns and can continuously learn from new security data without relying solely on predefined attack signatures.

With respect to the second research question, the findings showed that all three AI models investigated, Random Forest, Long Short-Term Memory (LSTM), and Autoencoder, were considered effective in detecting cyber threats. However, respondents rated the LSTM model as the most effective, followed by Random Forest, while Autoencoder ranked third. This suggests that deep learning techniques may achieve better performance in detecting sophisticated, previously unseen attacks than conventional machine learning algorithms. The superior performance of the LSTM model may be attributed to its ability to process sequential data and learn complex behavioral patterns within network traffic. This characteristic makes it particularly well-suited to identifying advanced persistent threats and zero-day attacks that often evade traditional detection methods. This finding is consistent with Kim et al. (2022), who reported that LSTM-based intrusion detection systems achieved higher detection accuracy and lower false alarm rates by modelling temporal relationships in cybersecurity data.

The effectiveness of the Random Forest model observed in this study also supports previous research. Although Random Forest performed

slightly below LSTM, respondents acknowledged its strong classification capability, high accuracy, and relatively easy implementation. This agrees with Sarker et al. (2021), who found that ensemble learning methods such as Random Forest remain reliable for detecting known cyberattack patterns while maintaining low computational complexity. Similarly, respondents agreed that Autoencoder models are effective for anomaly detection because they can identify deviations from normal network behaviour without requiring labelled datasets. However, the comparatively lower rating recorded for Autoencoder suggests that respondents considered its practical implementation more challenging than that of the other models. This observation corroborates the findings of Ferrag et al. (2022), who noted that although Autoencoders perform well in anomaly detection, their effectiveness depends largely on the quality and representativeness of the training data.

Overall, the findings demonstrate that Artificial Intelligence has become an indispensable component of modern cybersecurity systems. Nevertheless, the results also imply that AI should complement rather than replace conventional security mechanisms and human expertise. Effective cybersecurity depends not only on intelligent algorithms but also on skilled professionals who can interpret AI-generated alerts,

investigate incidents, and make informed security decisions. Consequently, organizations seeking to improve cybersecurity should adopt AI-based technologies while simultaneously investing in human capacity development, high-quality datasets, and robust cybersecurity policies to maximize the benefits of intelligent security systems.

Conclusion

This study evaluated the role of Artificial Intelligence (AI) in enhancing cybersecurity threat detection and response in Jigawa State, Nigeria. Based on the findings, it is concluded that AI makes a significant contribution to cybersecurity by improving the accuracy of threat detection, enabling real-time monitoring of network activities, reducing incident response time, detecting previously unknown cyber threats, and supporting automated incident response. These findings demonstrate that AI is an indispensable technology for strengthening modern cybersecurity operations.

The study also concludes that the AI models evaluated, Random Forest, Long Short-Term Memory (LSTM), and Autoencoder, are all effective in detecting cyber threats. However, the LSTM model emerged as the most effective among the three due to its superior ability to identify complex and evolving attack patterns, followed by Random Forest and Autoencoder. Therefore, integrating AI

models, particularly LSTM, with conventional cybersecurity mechanisms and the expertise of skilled cybersecurity professionals offers a more robust and effective approach to protecting digital systems against emerging cyber threats.

Recommendations

Based on the findings of this study, the following recommendations are made:

1. Organisations, educational institutions, and government agencies should strengthen the adoption of AI-based cybersecurity solutions to improve threat detection, real-time monitoring, incident response, and the identification of emerging cyber threats.
2. Governments and research institutions should invest in high-quality cybersecurity datasets and advanced AI algorithms to improve the accuracy, adaptability, and reliability of AI systems in detecting evolving cyber threats.
3. Governments and regulatory agencies should establish clear policies and ethical guidelines to ensure the transparent, accountable, secure, and responsible use of AI in cybersecurity while maintaining human oversight.
4. Organisations should prioritise the deployment of Long Short-Term Memory (LSTM) models for cybersecurity applications, as they demonstrated the highest effectiveness in detecting sophisticated and evolving cyber threats.

References

Arrieta, A. B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., García, S., Gil-López, S., Molina, D., Benjamins, R., Chatila, R., & Herrera, F. (2020). Explainable artificial intelligence (XAI): Concepts, taxonomies,

opportunities and challenges toward responsible AI. *Information Fusion*, 58, 82–115.

<https://doi.org/10.1016/j.inffus.2019.12.012>

Ashiku, L., & Dagli, C. H. (2021). Hybrid machine learning approach for intrusion detection systems. In *Proceedings of the IEEE Symposium Series on Computational Intelligence (SSCI)* (pp. 1–8). IEEE.

<https://doi.org/10.1109/SSCI50451.2021.9659943>

Biggio, B., & Roli, F. (2018). Wild patterns: Ten years after the rise of adversarial machine learning. *Pattern Recognition*, 84, 317–331.

<https://doi.org/10.1016/j.patcog.2018.07.023>

Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2022). Deep learning for cybersecurity intrusion detection: Approaches, datasets, and comparative study. *IEEE Communications Surveys & Tutorials*, 24(2), 1001–1038.

<https://doi.org/10.1109/COMST.2021.3054779>

Floridi, L., Cows, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P., & Vayena, E. (2018). AI4People—An ethical framework for a good AI society. *Minds and Machines*, 28, 689–707.

<https://doi.org/10.1007/s11023-018-9482-5>

Hozouri, A., Mirzaei, A., & Effatparvar, M. (2025). A comprehensive survey on intrusion detection systems with advances in machine learning, deep learning and emerging cybersecurity challenges. *Discover Artificial Intelligence*, 5, 314.

<https://doi.org/10.1007/s44163-025-00578-1>

- Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nature Machine Intelligence*, 1, 389–399. <https://doi.org/10.1038/s42256-019-0088-2>
- Kim, G., Lee, S., & Kim, S. (2022). A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. *Future Generation Computer Systems*, 126, 1–13. <https://doi.org/10.1016/j.future.2021.10.017>
- Mehrabi, N., Morstatter, F., Saxena, N., Lerman, K., & Galstyan, A. (2021). A survey on bias and fairness in machine learning. *ACM Computing Surveys*, 54(6), 115. <https://doi.org/10.1145/3457607>
- Mohamed, N. (2023). Current trends in AI and ML for cybersecurity: A state-of-the-art survey. *Cogent Engineering*, 10(1), 2272358. <https://doi.org/10.1080/23311916.2023.2272358>
- Papernot, N., McDaniel, P., Goodfellow, I., Jha, S., Celik, Z. B., & Swami, A. (2017). Practical black-box attacks against machine learning. In *Proceedings of the ACM Asia Conference on Computer and Communications Security (AsiaCCS)* (pp. 506–519). <https://doi.org/10.1145/3052973.3053009>
- Ring, M., Wunderlich, S., Scheuring, D., Landes, D., & Hotho, A. (2019). A survey of network-based intrusion detection datasets. *Computers & Security*, 86, 147–167. <https://doi.org/10.1016/j.cose.2019.101581>
- Sarhan, M., Layeghy, S., & Portmann, M. (2022). Towards a standard feature set for network intrusion detection systems. *IEEE Access*, 10, 10550–10566. <https://doi.org/10.1109/ACCESS.2022.3141234>
- Sarker, I. H. (2022). Machine learning: Algorithms, real-world applications and research directions. *Artificial Intelligence Review*, 55, 1–42. <https://doi.org/10.1007/s10462-020-09844-1>
- Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2021). Cybersecurity data science: An overview from machine learning perspective. *Journal of Network and Computer Applications*, 175, 102689. <https://doi.org/10.1016/j.jnca.2020.102689>
- Ullah, I., & Mahmoud, Q. H. (2021). A two-level flow-based anomaly detection model for IoT networks. *Computer Networks*, 191, 108236. <https://doi.org/10.1016/j.comnet.2021.108236>
- Verkerken, M., D’Hooge, L., Wauters, T., Volckaert, B., & De Turck, F. (2021). Towards Model Generalization for Intrusion Detection: Unsupervised Machine Learning Techniques. *Journal of Network and Systems Management*. 30. [10.1007/s10922-021-09615-7](https://doi.org/10.1007/s10922-021-09615-7).