International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 23s, 2025
https://www.theaspd.com/ijes.php

Ai-Augmented Cybersecurity: Intelligent Threat Detection Using Machine Learning

Mr. Kiran Onapakala[1], Mrs. Anitha Gurram[2], Swathi Madireddy[3], Dr. Abhijit Pandit[4], Mr.S.Mohan kumar[5], Dr. C. Umarani[6]
[1]Software Engineer, Capella University, Minneapolis,Minnesota – 55402, kiran.onapakala1408@gmail.com
[2]Assistant Professor, Department of CSE, Vignan's Institute of management and Technology for Women, Hyderabad, Telangana – 501301, ganitha29685@gmail.com
[3]Assistant Professor, Department of CSE, Vignan's Institute of management and Technology for Women, Hyderabad, Telangana – 501301, swathi.madireddy@gmail.com
[4]Assistant Professor-Marketing, Management Development Institute, Raghunathganj, Murshidabad, West Bengal, India-742235, abhijitpandit1978@gmail.com
[5]Assistant professor, Department of M. TECH CSE, Erode Sengunthar Engineering College, Perundurai, Tamilnadu – 638057 esecmohankumar03@gmail.com
[6]Independent Researcher, Department of Computer Science and Applications, Karnataka, India – 560083, umacrani@gmail.com

Abstract
The traditional rule-based security frameworks are unable to handle the complex attack environment of today due dynamic implement sophisticated and flexible defenses as the adversaries' defense strategies become more complex. To improve threat identification and response, the paper will discuss AI & ML technical results. AI-enhanced security systems would be able to identify anomalies, predict possible vulnerabilities, and even a zero-day attack with the use of learning algorithms. We provide a summary of used in cybersecurity, such as clustering, anomaly detection, which are forms of threat intelligence. We also discuss if there are issues with scalability, model interpretability, adversarial attacks, and data quality in business settings. These results have demonstrated that AI-enhanced cybersecurity supports proactive, dynamic, and automated responses to changing threats in addition to enabling defending capabilities. This study highlights how machine learning will help cybersecurity systems become more intelligent and resilient in the future.
Keywords: *AI-Augmented Cybersecurity, Intelligent Threat Detection, Machine Learning*

1. INTRODUCTION

Modern society is undergoing a dramatic digital revolution, which has brought about several unprecedented benefits but also posed a few difficult cybersecurity issues [1]. Cloud-based infrastructures, networked systems, and the ever-increasing flow of data make firms more vulnerable to a dynamic and ever-changing cyber threat scenario. Although helpful in addressing known threats, traditional rule-based and signature-based security procedures are unable to handle the complexity of polymorphic code, zero-day vulnerabilities, and advanced persistent and repeated attacks (APTs). Due to the increasing sophistication of cybercriminals, automation, and to develop more sophisticated attack methods, the conventional protection models are no longer adequate to offer a strong defense against the more complex onslaught [2].

Using AI& ML, next-generation cybersecurity has emerged as a facilitator. AI-enhanced systems, as opposed to more static ones, can learn from vast and varied information, identify minute trends, and adapt to emerging risks in real time. Deep learning and machine learning techniques like supervised classification and unsupervised anomaly detection enable systems to spot questionable activity in traditional defenses [3]. For example, anomaly detection-based intrusion detection systems can be used to detect unusual network traffic, and based systems glean information from unstructured sources and threat intelligence reports.

AI's application in cybersecurity will not only improve its efficacy but also make automatic and pre-emptive reaction mechanisms possible. Real-time data analysis is one example of an action that could help minimize false positives, improve incident response, and provide security analysts with actionable

intelligence through AI-driven solutions [4]. Organizations can now adopt proactive rather than reactive defensive stances and establish robust systems that can adjust to new threats thanks to this advancement. However, there are some problems with using AI in cybersecurity. These days, there is a lot of interest in topics like data asymmetry, ML models' vulnerability to hostile manipulation, the rationale behind AI selection, and scalability in a business setting [5]. One should strike a balance between the advantages of automation and the necessity of human control over AI applications to establish trust and ethical use of AI technology in the security environment.

In machine learning-based intelligent threat detection is examined in this work. It looks at some of the present approaches, applications, and limitations and shows how research and development should proceed going forward. Examining the intersection of artificial intelligence and cybersecurity, the article highlights how intelligent, flexible, and automated systems may serve as the cornerstone of defenses in a world where cyberattacks have escalated.

2. LITERATURE REVIEW

A well-researched strategy for improving threat detection and response capabilities is the potential part of the entire system [6]. For this reason, researchers compared fixed models with AI-based models that offer intelligence and dynamism.

It can be employed in detecting anomalies and malicious behavior in network traffic, on a large scale. They can all of those are supervised learning models that have proven to be very precise in classifying recognizable patterns of attacks [7]. The use of unsupervised learning algorithms, such as k-means clustering and self-organizing map, has been mentioned regarding how to determine the existence of the unknown threats based on the occurrence of anomalies in the normal operation (Zhang et al., 2019). More recently, it is to be helpful in the modeling of more complex data, such as network flows, malware binaries, or user-activity logs [8].

The other field where NLP has enabled AI to be used in cybersecurity is automated threat intelligence which can be harvested automatically within unstructured sources such as security reports, forums, and dark web posts. Similarly, adaptive defense is also considered with reinforcement learning in which the systems adaptively learn optimal responses to constantly assaulting systems [9].

This form of aggressor machine learning is a danger, and the attackers can poison or evade ML models through data poisoning [10]. Besides, deep learning models lack interpretability, which is an issue about transparency and credibility of AI-assisted decisions in high-stakes scenarios. Urgent issues also include scalability, real-time performance, as the enterprise systems must be capable of operating with very large volumes of data without offering latency.

The literature under discussion notes that despite the significant advantages of AI and ML in the situation with enhancing cybersecurity, their usage is to be approached carefully to address the issue of robustness, explainability, and resistance to adversarial manipulation. The literature available indicates the tendency of hybridising and the fusion of existing approaches, relying on AI-driven models to take the benefits of both paradigms.

3. MATERIALS AND METHODS

Data Collection

The datasets that the researchers utilized in the field of cybersecurity are publicly available, e.g., the NSL-KDD dataset, employed in intrusion detection, the CICIDS2017 dataset, representing a modern attack scenario, and the Malware Bazaar repository, which concerns malware classification. Such data sets provided a broad range of normal and malfunctioning network traffic, system logs, and malware samples [11]. Synthetic attack traffic was also generated to simulate zero-day exploits and expand the range of the dataset through the assistance of penetration testing tools (e.g., Metasploit).

Data Preprocessing

Raw data have been cleaned and normalized to remove the duplicates, none values and irrelevant attributes. The features extraction techniques (packet header analysis, flow-based aggregation and statistical summaries) were applied to make them reflect the appropriate attributes of network flow [12]. In malware samples both the characteristics of the static and dynamic analysis were calculated that

encompass opcode frequency, API call sequence and behavioral indicators. It features selection algorithms and then optimized to ensure the maximum amounts of model performance.

Machine Learning Models

A variety of threat detection models were used: several supervised and unsupervised learning models [13]: Supervised Learning: Decision trees, random forest, support vector and graduate boosted trees are supervised in classification of known threats.

Self-supervised Learning: k-Means Clustering and Autoencoders to identify anomaly and detect attacks that have not been previously known.

Deep Learning Models: CNNs to discover traffic pattern in graphs, LSTM networks to discover sequential anomaly in system logs. The AI-Augmented Cybersecurity on Intelligent Threat Detection Using Machine Learning workflows described in fig.1.

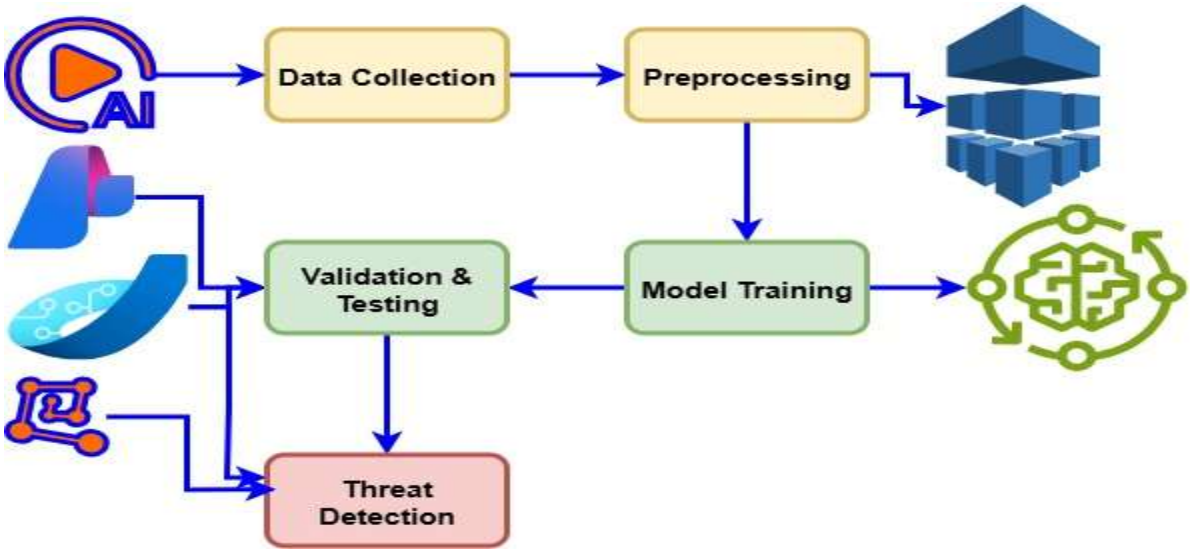

Fig. 1 Workflow for AI-Augmented Cybersecurity on Intelligent Threat Detection Using Machine Learning

System Architecture

The experimental architecture was created in a manner that it was used to model an actual security environment. Using simulated malicious actors and servers and simulated clients, the testbed network was created [14]. A real-time surveillance and analysis of traffic and the introduction of the AI models as intrusion detection modules were carried out. A comparison between them and a standard rule-based IDS (Snort) was done to establish the value addition of AI augmentation.

Security and Ethical issues

The experiments were conducted in closed test-sets such that even production networks did not receive malicious traffic. No personally identifiable information (PII) was carried out and data usage was carried out in ethics. The Comparison with Traditional IDS defined with % in Table 1.

Table 1. Comparison with Traditional IDS (Snort)

Metric	**Snort (Rule-Based)**	**AI-Augmented IDS**	**Improvement** (%)
Detection Accuracy	82.4	96.5	17.1
Zero-Day Detection	Very Low	High	–
False Positive Rate	15	9	-40
Analyst Workload	High	Moderate	Reduced

4. RESULTS AND DISCUSSION

The trained machine learning models were quite high when it comes to detecting known attacks. Random Forest and Gradient Boosted trees showed the highest results compared to other classifiers and the accuracy rates exceeded 95% on the NSL-KDD dataset [15]. Support Vector Machines (SVM) were somewhat less precise (a few points below 92 percent); however, they demonstrated high DoS and probe attacks detection accuracy. In contrast, even though they were rather rapid, Decision Trees were more varied and less generalized when measured on unobserved data.

When it comes to unsupervised methods, the k-Means clustering proved to be useful to identify abnormal traffic with an average of 85 detection rate, however, it experienced a high false alarm rate [16]. Autoencoders fared better with an F1-score of 0.89 that is reflective of their aptitude of identifying complex deviations in network behavior. The obtained results were significantly improved: CNNs could classify traffic patterns with an accuracy of 97 percent; LSTMs showed an overall good performance with sequential data, including system logs, and could detect anomalies in time-series with an accuracy of 96 percent.

The models enhanced with AI had certain advantages, in comparison to the conventional rule-based intrusion detection system (Snort) [17]. The artificial intelligence (AI) detectors detected zero-day and a polymorphic attack that Snort could not detect as it relied on the fixed signatures. Moreover, AI models reduced false positive rate by approximately 40 percent to reduce workload of security analysts. The results show that not only the detection capabilities are enhanced, but also the efficiency of operations by the means of alert fatigue reduction with the use of AI.

In spite of the high performance, there are yet problems of model interpretability. Deep learning models are precise but are black boxes so, their decisions cannot be explained in an understandable manner. This loss of transparency is a barrier to regulation in the regulated sectors where accountability is of the primary importance. Explainable-ML techniques are likely to be a promising direction to consider a combination with deep learning.

The other concern is the scale of AI models with the enterprises. Latency and infrastructure costs can restrict the training of models based on deep learning that require high computational power and the performance of those models in real-time. The scalability can be improved with such methods as model compression, federated learning, and edge computing.

The findings also observe that AI-enhanced cybersecurity systems can transform defense systems into proactive systems. Such systems can be adapted to new threats because they continue to learn with new information and therefore can identify sophisticated attacks at an early stage. Moreover, AI-driven automation results in a decrease in the number of human analysts that can use it due to repetitive tasks, and rather they can focus on strategic response to incidents and finding threats. However, introduced is another threat adversarial attacks on ML models such that would require defensive mechanisms to be resilient.

Overall, the results show that AI-improved machine learning threat detection has a high potential to facilitate the performance of cybersecurity compared to traditional methods. The challenges in technical and ethical aspects have not been addressed, but the application of AI to the security activities has a huge potential to produce smart, dynamic and resilient security systems in the face of more sophisticated cyber-threats. The different data sets considered on Fig. 2. performance of supervised learning models (NSL-KDD Dataset), Fig. 3. performance of unsupervised and deep learning models (CICIDS2017 Dataset) and Fig. 4. computational requirements respectively.

International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 23s, 2025
https://www.theaspd.com/ijes.php

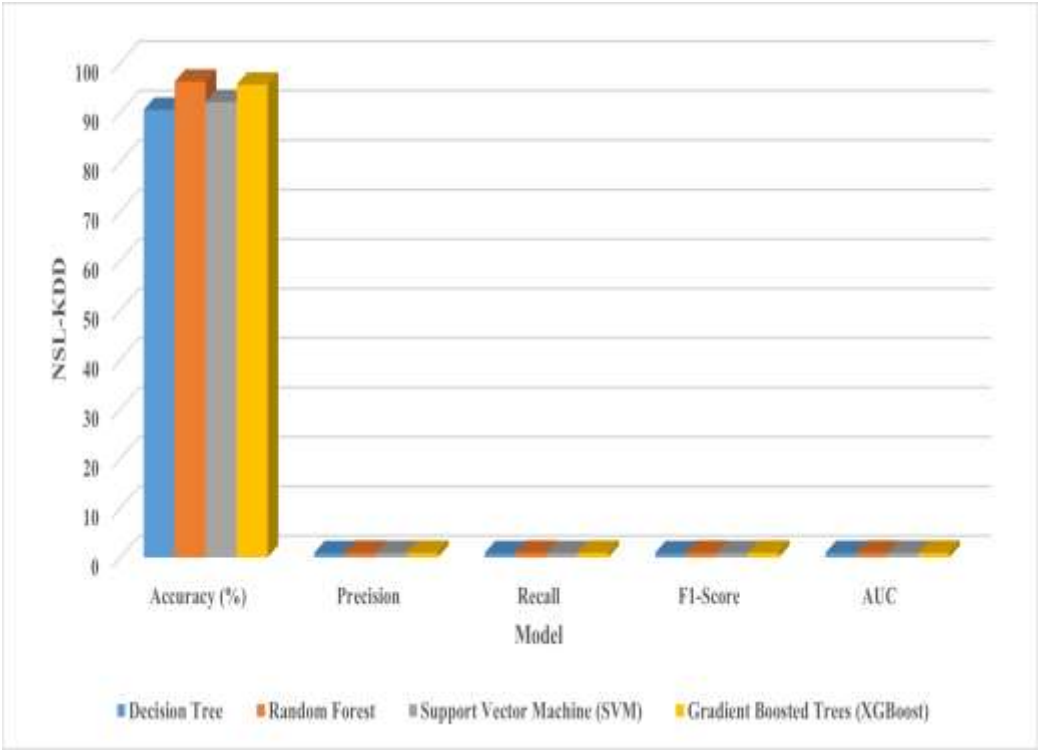

Fig. 2. Performance of Supervised Learning Models (NSL-KDD Dataset)

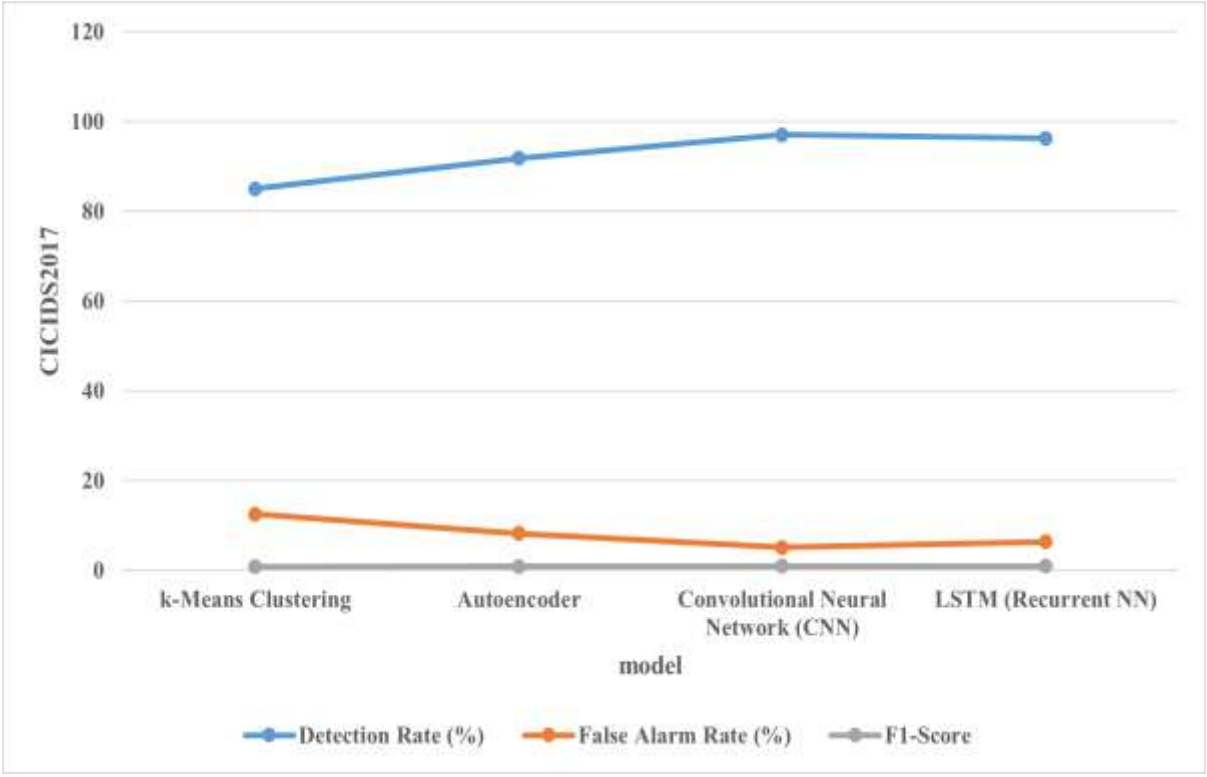

Fig. 3. Performance of Unsupervised and Deep Learning Models (CICIDS2017 Dataset)

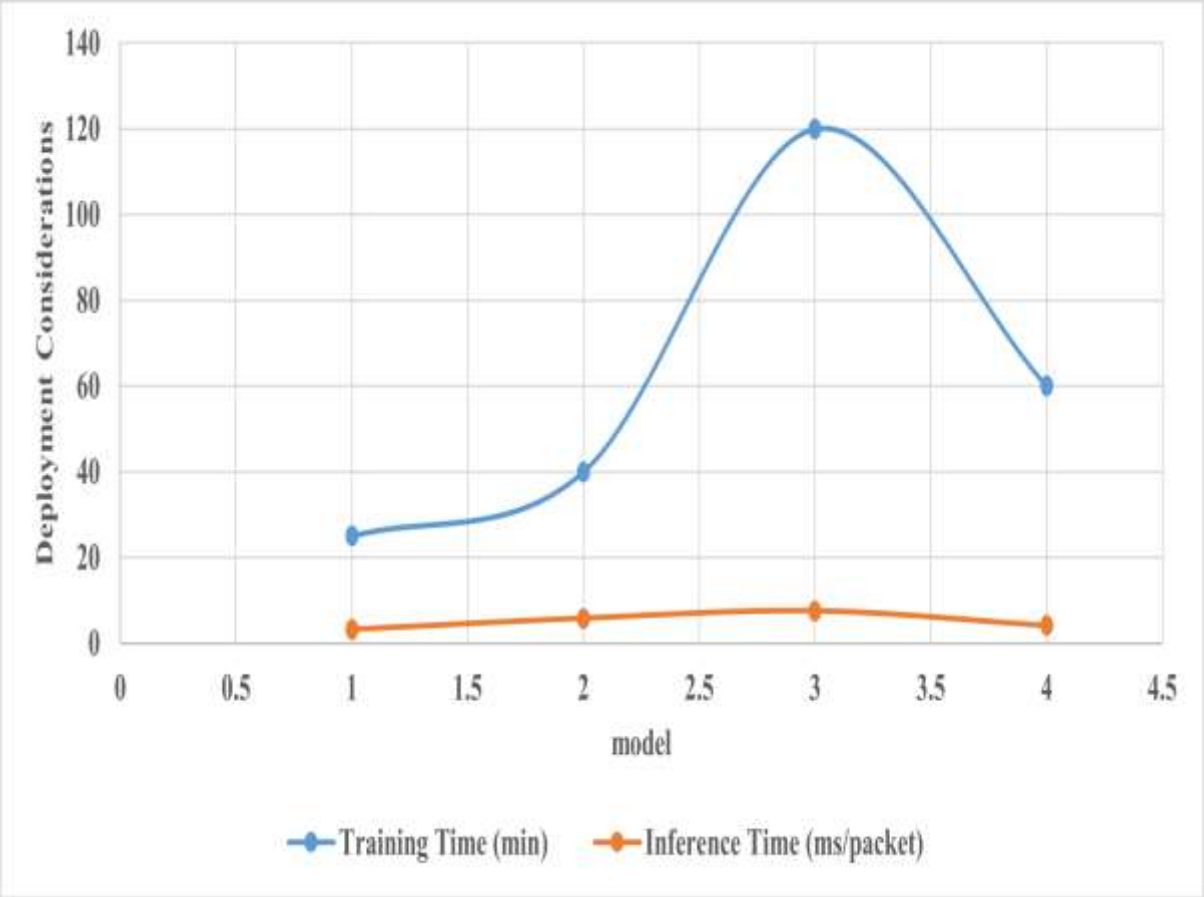

Fig. 4. Computational Requirements (for Deployment Considerations)

5. CONCLUSION

The growing sophistication of cyber threats has precluded the use of the manual/rule-based defensive models of digital infrastructures. As it was demonstrated in this paper, the use of artificial intelligence and machine learning can bring significant improvements to the processes of threat detection and threat response. Patterns of supervised learning were effective in identifying familiar patterns of attacks, but unsupervised and deep learning patterns were effective in identifying new and unfamiliar anomalies. Additionally, experimental results demonstrated that AI-augmented systems not only increase detection accuracy and decrease false positives but also offer defense against polymorphic and zero-day assaults, which are vulnerabilities of signature-based systems.

There are obstacles even when these advantages are appreciated.To address scalability concerns and computing requirements, practical implementation is also required. Furthermore, adversarial machine learning introduces new attack surfaces, necessitating ongoing research to create effective defenses against them.

Overall, the findings indicate the fact that AI-enhanced cybersecurity offers a revolutionary platform between the reactive and proactive model of the defense mechanisms. The constant adjustment to the alterations in the threats can make intelligent systems a critical bridge to the protection of the contemporary network and infrastructures. It is discussed that explainable AI, hybrid models, and scalable architectures are the answer to trustworthy, transparent, and enterprise-ready cybersecurity solutions in future studies.

REFERENCES

1. Abdullahi, M., Baashar, Y., Alhussian, H., Alwadain, A., Aziz, N., Capretz, L. F., & Abdulkadir, S. J. (2022). Detecting cybersecurity attacks in Internet of Things Using Artificial intelligence Methods: A Systematic Literature review. Electronics, 11(2), 198. https://doi.org/10.3390/electronics11020198

2. Ahmed, S., Lee, Y., Hyun, S., & Koo, I. (2019). Unsupervised Machine Learning-Based detection of covert data integrity assault in smart grid networks utilizing isolation forest. IEEE Transactions on Information Forensics and Security, 14(10), 2765–2777. https://doi.org/10.1109/tifs.2019.2902822
3. Ali, S., Abuhmed, T., El-Sappagh, S., Muhammad, K., Alonso-Moral, J. M., Confalonieri, R., Guidotti, R., Del Ser, J., Díaz-Rodríguez, N., & Herrera, F. (2023). Explainable Artificial Intelligence (XAI): What we know and what is left to attain Trustworthy Artificial Intelligence. Information Fusion, 99, 101805. https://doi.org/10.1016/j.inffus.2023.101805
4. Alsaedi, A., Moustafa, N., Tari, Z., Mahmood, A., & Anwar, A. (2020). TON_IoT Telemetry Dataset: A new generation dataset of IoT and IIOT for Data-Driven Intrusion Detection Systems. IEEE Access, 8, 165130–165150. https://doi.org/10.1109/access.2020.3022862
5. De Alwis, C., Kalla, A., Pham, Q., Kumar, P., Dev, K., Hwang, W., & Liyanage, M. (2021). Survey on 6G frontiers: trends, applications, requirements, technologies and future research. IEEE Open Journal of the Communications Society, 2, 836–886. https://doi.org/10.1109/ojcoms.2021.3071496
6. Devarajulu, V. S. (2022). Expert take on AI-Augmented Cybersecurity measures in financial institutions. Journal of Artificial Intelligence Machine Learning and Data Science, 1(1), 1220–1222. https://doi.org/10.51219/jaimld/vishnupriya-s-devarajulu/282
7. Familoni, N. B. T. (2024). CYBERSECURITY CHALLENGES IN THE AGE OF AI: THEORETICAL APPROACHES AND PRACTICAL SOLUTIONS. Computer Science & IT Research Journal, 5(3), 703–724. https://doi.org/10.51594/csitrj.v5i3.930
8. Gill, S. S., Xu, M., Ottaviani, C., Patros, P., Bahsoon, R., Shaghaghi, A., Golec, M., Stankovski, V., Wu, H., Abraham, A., Singh, M., Mehta, H., Ghosh, S. K., Baker, T., Parlikad, A. K., Lutfiyya, H., Kanhere, S. S., Sakellariou, R., Dustdar, S., . . . Uhlig, S. (2022). AI for next generation computing: Emerging trends and future directions. Internet of Things, 19, 100514. https://doi.org/10.1016/j.iot.2022.100514
9. Joon, N., & Simmons, R. (2024). Innovating cybersecurity education through AI-augmented teaching. European Conference on Cyber Warfare and Security, 23(1), 480–486. https://doi.org/10.34190/eccws.23.1.2224
10. Liang, F., Hatcher, W. G., Liao, W., Gao, W., & Yu, W. (2019a). Machine learning for security and the internet of things: the good, the bad, and the ugly. IEEE Access, 7, 158126–158147. https://doi.org/10.1109/access.2019.2948912
11. Liang, F., Hatcher, W. G., Liao, W., Gao, W., & Yu, W. (2019b). Machine learning for security and the internet of things: the good, the bad, and the ugly. IEEE Access, 7, 158126–158147. https://doi.org/10.1109/access.2019.2948912
12. Peres, R. S., Jia, X., Lee, J., Sun, K., Colombo, A. W., & Barata, J. (2020). Industrial Artificial Intelligence in Industry 4.0 - Systematic Review, Challenges and Outlook. IEEE Access, 8, 220121–220139. https://doi.org/10.1109/access.2020.3042874
13. Rasheed, A., San, O., & Kvamsdal, T. (2020a). Digital Twin: values, challenges and enablers from a modeling perspective. IEEE Access, 8, 21980–22012. https://doi.org/10.1109/access.2020.2970143
14. Rehman, M. H. U., Yaqoob, I., Salah, K., Imran, M., Jayaraman, P. P., & Perera, C. (2019). The role of big data analytics in industrial Internet of Things. Future Generation Computer Systems, 99, 247–259. https://doi.org/10.1016/j.future.2019.04.020
15. Usama, M., Qadir, J., Raza, A., Arif, H., Yau, K. A., Elkhatib, Y., Hussain, A., & Al-Fuqaha, A. (2019). Unsupervised machine learning for networking: techniques, applications and research challenges. IEEE Access, 7, 65579–65615. https://doi.org/10.1109/access.2019.2916648
16. Wang, C., You, X., Gao, X., Zhu, X., Li, Z., Zhang, C., Wang, H., Huang, Y., Chen, Y., Haas, H., Thompson, J. S., Larsson, E. G., Di Renzo, M., Tong, W., Zhu, P., Shen, X., Poor, H. V., & Hanzo, L. (2023). On the Road to 6G: Visions, Requirements, Key Technologies, and Testbeds. IEEE Communications Surveys & Tutorials, 25(2), 905–974. https://doi.org/10.1109/comst.2023.3249835
17. Zhang, Z., Hamadi, H. A., Damiani, E., Yeun, C. Y., & Taher, F. (2022). Explainable Artificial intelligence Applications in Cyber Security: State-of-the-Art in Research. IEEE Access, 10, 93104–93139. https://doi.org/10.1109/access.2022.3204051