Artificial Intelligence in Cybersecurity: Threats, Defenses, and Future Directions

Laylo Bakhronkulova
Research Scholar at AJOU University
Tashkent, Uzbekistan
laylo7883@gmail.com

Muhammad Ramzan Ali
Assistant Professor at AJOU University
Tashkent, Uzbekistan
Email: Ramzan.ali@ajou.uz

Zulfiya Khabirova
Associate Professor at AJOU Universit
Tashkent, Uzbekistan
Email: zulya.uz@gmail.com

Akimjonov Azimjon
Research Scholar at AJOU University
Tashkent, Uzbekistan
Email: stmustbk@gmail.com

Alimova Zebo
Research Scholar at AJOU University
Tashkent, Uzbekistan
Email: bb5911846@gmail.com

Abdumajidova Muslima
Research Scholar at AJOU University
Tashkent, Uzbekistan
Email:
muslimaabdumajidova23@gmail.com

***Abstract*— This study explores the usage of Artificial Intelligence and machine learning technology in modern cybersecurity. When cyberattacks becoming more frequent, organizations are turning to AI-powered solutions to improve their defense systems. Adoption of AI technologies like machine learning and deep learning is shown to improve the accuracy of threat detection, but data reliability, model interpretability, and bias in decision-making systems remain significant issues. Research has proven AI to be most successful in preventing large-scale attacks, i.e., DDoS, through the recognition of patterns in network traffic based on models like Recurrent Neural Networks (RNNs) and Convolutional Neural Networks (CNNs). The application of AI technologies, such as machine learning and deep learning, has been shown to improve the speed and precision of threat detection so that it becomes easier to identify and counteract previously unknown vulnerabilities. Despite these advantages, very low rates of organizations have fully implemented AI-driven security solutions, and confidence in AI decision-making still affects deployment. This article also highlights increasing incidents of AI-driven cyber attacks, such as AI-created malware, automated phishing, and deepfake identity theft, that are outrunning traditional security controls. This analysis also emphasizes the growing importance of application of AI in cybersecurity with underscoring its potential to strengthen defens systems against zero-day attacks and similar evolving threats. However, it also reviews some of the challenges that need to be addressed for more effective integration of AI models in cybersecurity, such as the reliability of the data that is being used for its' training. With the development in AI technologies, machine learning based models are expected to play an increasingly crucial role in protection of both businesses and individuals from sophisticated cyberattacks. And despite all the advantages, the full implementation of AI-driven security solutions remains low. What is more, concerns about the trustworthiness of AI decisions and the lack of transparency in AI models still remains.**

Keywords*— *Cybersecurity, Deep Learning, Anomaly Detection, Intrusion Prevention, Machine Learning, Neural Networks, Cyber Threats, Artificial Intelligence, Network Security, Adversarial Attacks.

I. INTRODUCTION

This article will systematically summarize how deep learning can be used to increase the security of cyberspace, especially in fields like intrusion prevention and anomaly detection and what kind of situation we already have in the world of IoT regarding the usage of AI and machine learning in cybersecurity.

Nowadays, network traffic has become so complex that only deep learning stands a chance of learning these intricate patterns. Its methodological advantage is in having the capacity not to be a sink for extra data, but to tackle new information with aplomb. Different architectures of deep learning Convolutional Networks (CNNs), Recurrent Neural Networks (RNNs), Autoencoders, and Generative Adversarial Networks (GANs)(see them all at work in the chapters above) are considered with the reasons for their ability to handle high-dimensional data and detect anomalies across different domains of cybersecurity provisos [16].The deep learning's advantages in anomaly detection are particularly marked in unsupervised

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol2.8592

scenarios. In these favourable frames, it can seek to discern tiny departures from the norm of datasets without using labelled instances to guide its decisions. In its intrusion detection and prevention systems (IPS), deep learning improves the ability to identify and prevent attacks. As it is able to classify network traffic based on many different parameters, the accuracy of such systems increases while false positives decrease. But unanswered questions loom ahead, such as the need for big, high-quality databases that could be targets of adversarial attacks on systems and models' expansibility. This is an area where neither deep learning technology nor its applications have yet developed mature responses [26].

II. Materials and methods

A. Literature review

According to literature on deep learning in cybersecurity, it seems that all agree its potential to transform the fields of anomaly detection and intrusion prevention systems (IPS) is already evident. Traditional approaches like signature-based intrusion detection systems (IDS) are losing their effectiveness as cyberattacks are constantly evolving. Especially with zero-day exploits, which evade detection by such traditional methods [25]. In the face of increasingly sophisticated cyber threats, deep learning, with its unique capability to adapt and learn from large datasets, gives hope for the future. Thoroughly-trained deep learning models, such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Autoencoders and generative adversarial networks (GANs), have already been put to use successfully in cybersecurity tasks including anomaly detection and intrusion prevention. These models are excellent at identifying complex patterns and revealing tiny discrepancies; especially in high-dimensional and time-series data, such as network traffic or system logs produced over years [4]. For example, on time series data, RNNs have proved effective at learning temporal dependencies in the data and identifying anomalous peaks [22] while autoencoders used to distinguish between normal data representations. However, challenges remain such as the need for high-quality labelled datasets and interpretability of models [21]. Nevertheless, deep learning has achieved tangible success in real-world applications: intrusion detection in IoT networks, cloud security, and malware detection. Currently active research is concerned with improving model accuracy, reducing computational costs, and improving interpretability to increase the uptake of deep learning models in cybersecurity as a whole [26].

B. The Evolving Landscape of Cybersecurity Threats

The digital space is increasingly complex and the frequency of cyberattacks ever-on-the-rise. These attacks include everything from basic denial-of-service (DoS) attempts to highly sophisticated, concerted breaches meant to siphon valuable or harmful data or otherwise cause havoc on (or to) mission-critical infrastructure. Signature-based intrusion detection systems (IDSs), which detect known attack patterns are becoming less effective against the evolving threat landscape. As it turns out, signature-based solutions are only as good as they are at discovering new attacks; malicious actors have the capability to continuously adjust their techniques to facilitate new attacks, leading to attacks being adapted and re-used with new techniques that signature-based solutions simply was not designed to recognize. These attacks, known as zero-day exploits, target unknown vulnerabilities, making signature-based IDSs ineffective [25]. Additionally, the amount of network traffic generated is large, and the complexity of modern systems makes it harder for traditional methods to effectively analyse data and find malicious behavior interspersed among all the background noise. Meanwhile, these legacy approaches have their limitations [1]; increasing need for advanced, intelligent security systems that can classify both known and unknown threats [1]. Deep learning has the potential to learn complex patterns and adapt to new data, making it an exciting approach to tackle these shortcomings.

C. Deep learning Fundamentals in Cybersecurity

A sub-field of machine learning known as deep learning employs artificial neural networks with multiple layers to discover high-level abstractions in raw data. In cybersecurity, data tends to be high-dimensional and complex, making this ability of hierarchical representation learning inherently useful. Due to the strength of this technology several deep learning architectures have shown to be efficient in the entire for the cybersecurity area. Convolutional neural networks (CNNs) are specialized in handling structured data, such as images and network traffic patterns, and are very proficient in revealing spatial relationships and features in them [16]. Long short-term memory (LSTM) networks and gated recurrent units (GRUs), which are types of recurrent neural networks (RNNs), are designed to deal with sequential data, making them ideal candidates for time-series data such as network log or events that have temporal dependencies [13]. Autoencoders are unsupervised learning models that are particularly good at identifying anomalies by learning a compressed version of normal data (s) and flagging instances which vary significantly from this learned version [19]. On the other hand, generative adversarial networks (GANs) may produce synthetic data which can extend small datasets and enhance other deep learning models. These architectures are selected because their flexibility and pattern recognition abilities allow them to cope well with new dynamic and evolving threats in the fields of cybersecurity [28].

D. Anomaly Detection using Deep Learning

Anomaly detection, which refers to identifying unusual patterns or deviations from expected behaviour, is an important part of cybersecurity. Deep learning still provides large advantages over, for example, traditional methods in the potential to surf through complex datasets and spot slight discrepancies. In the case of anomaly detection in cybersecurity, with the presence of classified and unclassified data, the unsupervised and semi-supervised deep learning techniques are well suited to cybersecurity use cases since you can train on unlabelled and partially labelled data, which is a subject we discuss in our Summary [19]. For instance, given a normal network traffic, an autoencoder is trained to learn its compressed representation. It then flags these deviations from the representation, which signify classical activities, as anomalies. Data learned from the logs of normal execution flows, used with deep learning models, can detect unexpected events or sequences of events possibly indicating malicious activity [27]. Deep learning for anomaly detection has been successfully applied not only for network traffic and system logs but also for user behaviour analysis, unusual access pattern detection, and anomaly detection of other data streams. Deep learning models such as recurrent neural networks (RNN) can be used to present the temporal dependencies of the signal and highlight abnormal behaviours changing over time in time series data. Yet some challenges remain, such as the existence of high-dimensional data and understanding the model outputs. More advanced deep learning architectures and more effective techniques are being investigated to bring the accuracy and explainability of deep networks up to closer limits, thus allowing their deployment in many applications [29].

E. Intrusion Prevention Systems (IPS) Enhanced by Deep Learning

Intrusion Prevention Systems (IPS) are essential in modern cybersecurity world, as they permanently monitor and check a network traffic to identify anomalies and block potential threats. Traditionally, IPS uses signature-based and heuristic methods to detect already known attack patterns. However, these conventional techniques often have difficulty recognizing new or evolving cyber threats, like zero-day attacks. To overcome these challenges, machine learning, especially deep learning, has proven to be a good method for improving the capabilities of IPS technology [1].

Deep learning-based IPSs leverage advanced neural network architectures to analyze vast amounts of network traffic in real time. Unlike traditional IPSs, which rely on predefined rules, deep learning models can autonomously learn from historical and already collected data to identify different patterns of suspicious behavior and therefore predict new patterns a well. These systems utilize various features, including packet headers, payload contents, and network flow characteristics, to classify incoming traffic as benign or malicious [5]. This ability makes deep learning-powered IPS capable to adapt to enhancing threats and attack patterns dynamically identifying those schemes that were previously unknown .

Neural networks commonly used for IPSs include deep neural networks, convolutional neural networks (CNNs), recurrent neural networks (RNNs), long short-term memory networks (LSTMs), autoencoders, and generative adversarial networks (GANs). CNNs have proven to be effective in extracting features from network packets, whereas RNNs and LSTMs are especially adept at identifying attack strategies that depend on time. Autoencoders and GANs are capable of identifying anomalies by learning standard traffic patterns and highlighting signs of intrusions [9].

Incorporating deep learning into Intrusion Prevention Systems (IPSs) offers many benefits, especially in enhancing detection precision. Conventional rule-based systems often produce a high volume of false positives, which demands ongoing manual adjustments to prevent unwarranted and baseless interruptions such as those made by hackers or other interrupters [14]. In contrast, deep learning models can highly minimize false positives by recognizing nuanced differences between legitimate behavior and harmful traffic patterns that may mean intrusions into the system and subsequent loose of data [16]. What is more, IPSs that utilize deep learning can manage and control substantial amounts of network data, making them well-suited for high-traffic settings like corporate or governmental networks and cloud infrastructures or other systems that permanently store a huge amount of private information [14][28][29].

A significant benefit of deep learning-based intrusion prevention systems (IPSs) is their capability to identify zero-day attacks, which are threats that have not been previously recognized and lack established signatures. In contrast, traditional IPSs depend on threat databases that are updated manually, creating a vulnerability gap until new attacks are detected [22][30]. Deep learning models can learn from past attack patterns and predict new variations, offering a proactive defense against new cyber threats [22].

Nonetheless, these systems face various challenges, with a significant concern being the considerable computational expense. Deep learning models demand a lot of processing power, particularly in high-bandwidth environments where prompt threat detection is crucial. Training and deploying such models always require modern and specialized hardware like graphics processing units (GPUs) or tensor processing units (TPUs), which can increase both the cost and complexity of implementation [2].

One of the challenges faced is the necessity for ongoing retraining. Cyber threats are constantly changing, and attackers often create new methods to circumvent current security protocols [14]. To stay effective, deep learning models need to be regularly updated with new data to identify emerging attack vectors. However, obtaining high-quality labeled data for training is a complex issue, as cybersecurity datasets frequently exhibit class imbalances, with benign traffic far outnumbering malicious samples. This problem might result in biased models that have difficulty detecting rare but highly significant attacks [13][26].

The future of deep learning-enhanced IPSs lies in hybrid security models, where deep learning is integrated with traditional security techniques to create more adaptive and reliable intrusion prevention mechanisms. Combining deep learning with rule-based systems, threat intelligence feeds, and behavioral analytics can create a multi-layered defense strategy capable of addressing a wide range of cyber threats [29].

In summary, deep learning has greatly improved the functionality of contemporary IPSs, providing enhanced accuracy, flexibility, and the ability to identify previously unknown threats. Nonetheless, issues such as computational demands, adversarial attacks, and the necessity for ongoing retraining need to be tackled to fully harness the advantages of deep learning in IPSs. As cyber threats continue to advance, the adoption of AI-driven IPS solutions will be increasingly vital for protecting digital infrastructure from complex cyberattacks.

F. Materials

To obtain a comprehensive and reliable data about the current situation of cybersecurity and the use of AI and machine learning technologies in this area we will use a range of different sources. A significant resource for this analysis is an open source article by Jacob Fox published on the Cobalt platform on October 10, 2024 [12]. This research provides information about the impact of AI on contemporary cybersecurity, especially how machine learning algorithms help in detecting and addressing new cyber threats. It provides a detailed statistics of different challenges of implementing AI-based security solutions in corporative environments. This article serves as a crucial foundation for understanding trends in use of AI throughout the world.

Additionally, we will refer to a scientific study made by the Check Point online platform team on October 18, 2024 [6]. This study offers a statistical analysis of cybersecurity threats recorded over the year, highlighting notable trends such as the rise of zero-day attacks and DDoS incidents in different parts of the world. It also provides information about how different organizations are integrating AI and machine learning to protect from these threats and offers some statistics about the effectiveness of various AI-driven security strategies.

Except these sources, we will also include data from various cybersecurity research papers and industry reports that cover essential topics like IDSs, IPSs and AI-enhanced network security solutions. Special attention will be given to studies that focus on the use of deep learning technologies, such as RNNs and CNNs. These studies provide valuable data and elaborate into how AI can improve security systems by detecting suspicious patterns in network traffic and enhancing the accuracy of real-time threat detection.

What is more, to fully understand all the challenges related to AI integration in cybersecurity, we will review reports that discuss issues like data reliability, model interpretability and bias in AI-driven decision-making systems [21]. By examining different viewpoints on some challenges, we are going to present a balanced perspective on both benefits and limitations of the use of AI in the cybersecurity field. By comparing information from Jacob Fox's article on the Cobalt platform and the cybersecurity statistical analysis by Check Point Research, we are going to develop a comprehensive understanding of the role of AI for data protection in modern days. [6],[12].

G. Analysis

In recent years, AI became an advanced tool for data protection and privacy, gaining popularity among lots of cybersecurity experts. A study by the Ponemon Institute found that around 70% of participants believe that AI is highly effective in identifying previously unknown threats [12]. What is more, 53% of security experts noted that their organizations still are only implementing AI-based security solutions that use machine learning techniques [12]. This increasing dependence on AI is vital, especially as the number of cyber threats targeting businesses globally continues to rise. Zero-day attacks especially are significant financial and security threats as cyberattacks have seen a dramatic rise in recent years [6]. Research from "Check Point Research" indicates a 75% increase in cyberattacks throughout the world during the third quarter of 2024 [6]. Such techniques as machine learning and deep learning are particularly highly effective in large-scale attacks, including DDoS attacks in software-defined networks [24]. Deep learning technologies, such as RNNs and CNNs, have already proven their capability to analyze network traffic and recognize suspicious behavior patterns [9]. For example, research emphasized the success of an Attentional LSTM-CNN model in identifying anomalies in quasi-periodic time series data, significantly enhancing cybersecurity threat detection [22].

Despite the rapid enhancement of AI in the cybersecurity field and studies indicating that AI can greatly improve the accuracy of IDSs, only 18% of organizations have fully integrated AI-based security systems in their infrastructures [12]. Experts have examined the latest developments in machine learning and deep learning techniques applied to IDS while also admitting the existence of some challenges that these systems may encounter [5]. Additionally, a study has introduced the PS-IPS framework—an Intrusion Prevention System that utilizes machine learning on programmable switches. This innovation enhances adaptability and efficiency, making it especially beneficial for securing critical infrastructures, such as energy grids, industrial control systems, and financial institutions [20]. Whilst AI-driven cybersecurity solutions are advancing, several challenges still persist. A primary concern is ensuring the reliability and trustworthiness of the data used to train AI models, and the interpretability of AI-driven decisions poses a significant issue, as opaque "black-box" models can lead to false positives or missed threats [21][15].Despite these obstacles, the future of AI in cybersecurity appears to be bright. Research suggests that the integration of AI and machine learning will further enhance threat detection methods, automate network traffic analysis, and strengthen defenses against zero-day attacks [23]. As AI models become more advanced and transparent, their role in cybersecurity is expected to expand in the future, providing stronger and better protection for both businesses and individuals [23].

In the third quarter of 2024, an average of approximately 1,870 cyberattacks per company were recorded, showing a 75% increase compared to the same quarter in the year 2023 and a 15% rise compared to the second quarter of 2024. Simultaneously, around 74% of security professionals reported that their organizations suffer from cyberattacks involving artificial intelligence, whilst 75% of experts stated that they were forced to adjust their security strategies to better combat AI-driven cyber threats. The most heavily impacted regions were African countries, experiencing over 3,000 attacks per week throughout 2024, nearly 50% more than in 2023. [12][6]

Despite the increasing adoption of AI in cybersecurity, its inherent characteristics—such as easy access to shared data and system control—raise concerns. 63% of security professionals reported that they use AI primarily to create rule sets that reflect known security patterns and indicators (Ponemon Institute)[12]. Additionally, 50% stated that they use AI exclusively for training purposes. Furthermore, 85% of researchers agree that only machine intelligence-based technologies are capable of detecting and preventing AI-generated threats. [12]

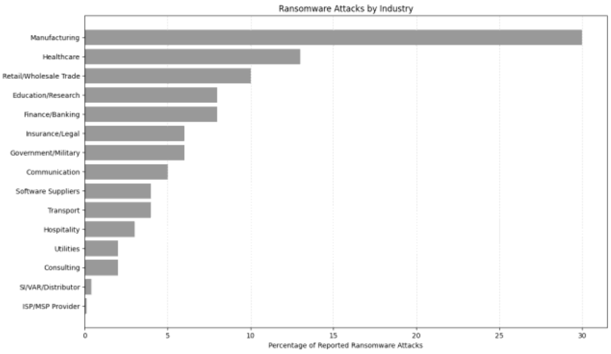

Fig 1. Statistics of ransomware attacks in 2024.

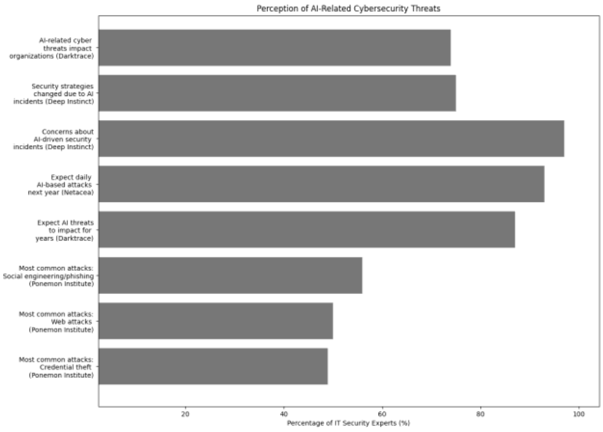

Fig 2. Perception of AI-related Cybersecurity Threads in 2024.

III. Results and discussion

While a review of recent research actually confirms the growing role of AI in both offensive and defensive cybersecurity trends, there are several important considerations to keep in mind when comparing the findings to technical specifications. For a more accurate comparison, we have presented a comparative table of deep learning models in cybersecurity which is represented as Table 1

Firstly, we can agree with the emphasis in the literature [13],[27] on the superior pattern recognition ability of deep learning algorithms in intrusion detection tasks. This is well aligned with the information given in Table 1, which shows that hybrid models offer high accuracy and performance for classification tasks. However, the literature often overlooks the practical limitations of these models — particularly in terms of resource consumption and inability to generalize well to temporal data.

Moreover, while RNN-based models such as LSTM and GRU are often praised for their ability to handle temporal sequences (e.g., system logs), although it is worth noting that they are difficult to train and suffer from vanishing gradient problems. This calls into question their scalability in real-time cybersecurity systems that must handle huge amounts of streaming data.

The application of unsupervised models, including autoencoders and GANs, is widely recognized for anomaly detection [16], [21]. Autoencoders are ideal for detecting outliers without labeled data. Nevertheless, it is worth avoiding over-reliance on such models due to their low interpretability, which is still a problem in environments where explainability is crucial, such as in the government or financial sector.

From Table 1 which presents advantages and disadvantages of various types of models with their application fields we can determine that recurrent neural networks (RNNs) such as LSTM and GRU are best suited for temporal dependency tasks, e.g., system log event analysis. RNNs are hard to train and suffer from vanishing gradients, restricting their stability and scalability. Autoencoders enable unsupervised learning along with outlier detection by means of abnormality detection. Yet they are low in interpretability and highly reliant upon the quality of data on which they are learned. GANs can potentially solve the class imbalance problem by creating synthetic instances and therefore improve the resilience of other models. They do, however, need a significant amount of computational power and are prone to training instability. Fully connected networks offer extremely high accuracy for classification problems and rather simple structures. They are not effective in learning long-term temporal patterns in the data and therefore are weaker in more complicated cases. Hybrid models, e.g., combinations of RNN and CNN, have the most potential. Such models can jointly process spatial and temporal features, which is particularly beneficial when faced with constantly changing threats. They need to be properly tuned and can be resource-intensive.

Overall, while existing research provides a solid foundation for understanding the role of AI in cybersecurity, it tends to overexaggerate the benefits while omitting or underestimating the practical limitations associated with implementing the models themselves. A more nuanced perspective - balancing, performance, interpretability, and resource requirements - is critical to creating effective and realistic defense systems, as shown in Table 1. Lastly, strategic selection and tuning of AI models depending on the nature of cyber threats and data are required in creating an effective defense mechanism. Hybrid models particularly possess immense potential in offering overall analysis and high accuracy of threat detection.

IV. Acknowledgments

We would like to express our heartfelt gratitude to the researchers, cybersecurity experts, and data scientists whose extensive efforts and pioneering research have significantly enhanced our understanding of deep learning applications in cybersecurity. Their commitment to advancing knowledge in artificial intelligence, threat detection, and risk management has been crucial in creating innovative solutions to address contemporary cyber threats. The methodologies, case studies, and experimental results they have shared have laid the foundation for further investigation and development in this rapidly changing field. We also wish to express our sincere appreciation to the various academic institutions, government agencies, private organizations, and research centers that have provided essential funding, infrastructure, and technical support for the studies mentioned in this paper. Their steadfast dedication to promoting research in cybersecurity and artificial intelligence has been crucial in driving new discoveries and improving existing methods to strengthen the security and resilience of digital systems. We also acknowledge the collaborative efforts of interdisciplinary teams, industry professionals, and practitioners who have worked diligently to connect theoretical advancements with practical cybersecurity applications. Their knowledge, insights, and contributions have been crucial in transforming AI-driven security innovations into practical solutions that safeguard organizations, governments, and individuals from new cyber threats. Furthermore, we recognize the ongoing efforts of open-access platforms, publishers, and peer reviewers who have promoted knowledge sharing and ensured that the latest research is accessible to the global cybersecurity community. The advancements in incorporating artificial intelligence into cybersecurity frameworks would not have been possible without the collective dedication of these individuals and organizations. We express our heartfelt thanks to everyone who has played a role in this field and anticipate further progress driven by their expertise and commitment to innovation in the future.

Table 1: Comparative Table of Deep Learning Models in Cybersecurity

Model Type	**Application (Anomaly Detection/ Intrusion Prevention)**	**Advantages**	**Disadvantages**
CNN	Both	Also used for effective feature extraction, high accuracy in processing structured data like images and network traffic patterns. Detect spatial relationships and features well	Common challenges with machine learning models: Computationally intensive, require large datasets, not very good with sequential data.
RNN (LSTM, GRU)	Both	Effective for sequential data, retains temporal dependencies, good for time-series analysis such as network logs or system events	Hard to train, computational complexity, gradients can vanish.
Autoencoders	Primarily Anomaly Detection	Unsupervised learning, which is used when no labelled data is available, can also be used to find outliers; this process involves learning a compressed representation of normal data and alerting the system in case of deviations.	Reconstruction error is a complex metric that gives little insight, excellent performance relies heavily on the quality of normal data used to train.
GANs	Both	Trained on data until October 2023, Generates synthetic data to help tackle data imbalance problems to use and can also improve the robustness of certain deep learning models by polling data sets.	Training instability: High computational cost: Hard to train/evaluate.
Deep Feedforward Networks	Intrusion Prevention	Fairly simple architecture, high accuracy with a lot of training data, good for classification tasks.	Tend not to encode complex relationships over long time periods, may overfit more easily without sufficient regularization.
Hybrid Models (e.g., CNN-LSTM)	Both	It captures spatial and temporal features simultaneously which are key in complex cybersecurity use cases, utilizing the all strengths of CNN and RNN.	More complexity, more computational cost, needs proper design and tuning.

V. REFERENCES

[1] A. Abdallah, A. Alkaabi, G. Alameri, S. H. Rafique, N. S. Musa, and T. Murugan, "Cloud network anomaly detection using machine and deep learning techniques—recent research advancements," IEEE Access, vol. 12, pp. 56749–56773, 2024. [Online]. Available: https://doi.org/10.1109/ACCESS.2024.3390844.

[2] M. Z. Alom, T. M. Taha, C. Yakopcic, S. Westberg, P. Sidike, M. S. Nasrin, M. Hasan, B. C. Van Essen, A. A. S. Awwal, and V. K. Asari, "A state-of-the-art survey on deep learning theory and architectures," Electronics, vol. 8, no. 3, p. 292, 2019. [Online]. Available: https://doi.org/10.3390/electronics8030292.

[3] T. Al-Shehari, et al., "Enhancing insider threat detection in imbalanced cybersecurity settings using the density-based local outlier factor algorithm," IEEE Access. [Online]. Available: https://ieeexplore.ieee.org/document/10459083.

[4] V. Barba-Sánchez, et al., "Effects of digital transformation on firm performance: The role of IT capabilities and digital orientation," Heliyon, vol. 10, no. 6, 2024. [Online]. Available: https://pubmed.ncbi.nlm.nih.gov/38509885/.

[5] K. Bathiri and M. Vijayakumar, "Enhancing intrusion detection system (IDS) through deep packet inspection (DPI) with machine learning approaches," in 2024 International Conference on Advances in Data Engineering and Intelligent Computing Systems (ADICS), IEEE, 2024. [Online]. Available: https://ieeexplore.ieee.org/document/10533473.

[6] Check Point Research, "A closer look at Q3 2024: 75% surge in cyber attacks worldwide," Check Point Blog, Feb. 24, 2025. [Online]. Available: https://blog.checkpoint.com/research/a-closer-look-at-q3-2024-75-surge-in-cyber-attacks-worldwide/.

[7] F. Cerasuolo, et al., "Adaptive intrusion detection systems: Class incremental learning for IoT emerging threats," in 2023 IEEE International Conference on Big Data (BigData), IEEE, 2023. [Online]. Available: https://ieeexplore.ieee.org/document/10386129.

[8] S. Chakraborty, et al., "Interpretability of deep learning models: A survey of results," in IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), IEEE, 2017. [Online]. Available: https://doi.org/10.1109/UIC-ATC.2017.8397411.

[9] J. N. Chukwunweike, M. Yussuf, O. Okusi, T. O. Bakare, and A. J. Abisola, "The role of deep learning in ensuring privacy integrity and security: Applications in AI-driven cybersecurity solutions," World Journal of Advanced Research and Reviews, vol. 23, no. 2, pp. 2550, 2024. [Online]. Available: https://doi.org/10.30574/wjarr.2024.23.2.2550.

[10] X. D. Do, H. D. Nguyen, and V. N. Tisenko, "Malicious URL detection based on machine learning," International Journal of Advanced Computer Science and Applications, vol. 11, no. 1, 2020. [Online]. Available: https://doi.org/10.14569/IJACSA.2020.0110119.

[11] H. N. Fakhouri, et al., "A comprehensive study on the role of machine learning in 5G security: Challenges, technologies, and solutions," Electronics, vol. 12, no. 22, p. 4604, 2023. [Online]. Available: https://doi.org/10.3390/electronics12224604.

[12] J. Fox, "Top 40 AI cybersecurity statistics," Cobalt Blog, Oct. 10, 2024. [Online]. Available: https://www.cobalt.io/blog/top-40-ai-cybersecurity-statistics.

[13] H. Gonaygunta, et al., "Enhancing cybersecurity: The development of a flexible deep learning model for enhanced anomaly detection," in 2024 Systems and Information Engineering Design Symposium (SIEDS), IEEE, 2024. [Online]. Available: https://doi.org/10.1109/SIEDS61124.2024.10534661.

[14] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," Computer Networks, vol. 169, p. 107094, 2020. [Online]. Available: https://doi.org/10.1016/j.comnet.2019.107094.

[15] S. R. Hong, J. Hullman, and E. Bertini, "Human factors in model interpretability: Industry practices, challenges, and needs," Proceedings of the ACM on Human-Computer Interaction, vol. 4, no. CSCW1, pp. 1–26, 2020. [Online]. Available: https://doi.org/10.1145/3392878.

[16] R.-H. Hwang, M.-C. Peng, C.-W. Huang, P.-C. Lin, and N. Nguyen, "Unsupervised deep learning model for early network traffic anomaly detection," IEEE Access, vol. 8, pp. 30387–30399, 2020. [Online]. Available: https://doi.org/10.1109/ACCESS.2020.2973023.

[17] J. M. Kaplan, et al., Beyond cybersecurity: Protecting your digital business. Hoboken, NJ: Wiley, 2015.

[18] A. R. Khan, M. Kashif, R. H. Jhaveri, R. Raut, T. Saba, and S. A. Bahaj, "Deep learning for intrusion detection and security of Internet of Things (IoT): Current analysis, challenges, and possible solutions," Security and Communication Networks, vol. 2022, p. 4016073, 2022. [Online]. Available: https://doi.org/10.1155/2022/4016073.

[19] G. Kocher and G. Kumar, "Machine learning and deep learning methods for intrusion detection systems: Recent developments and challenges," Soft Computing, vol. 25, no. 15, pp. 9731–9763, 2021. [Online]. Available: https://www.researchgate.net/publication/352725425_Machine_learning_and_deep_learning_methods_for_intrusion_detection_systems_recent_developments_and_challenges.

[20] A. Y.-P. Lee, et al., "PS-IPS: Deploying intrusion prevention system with machine learning on programmable switch," Future Generation Computer Systems, vol. 152, pp. 333–342, 2024. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4440724 .

[21] W. Liang, et al., "Advances, challenges, and opportunities in creating data for trustworthy AI," Nature Machine Intelligence, vol. 4, no. 8, pp. 669–677, 2022. [Online]. Available: https://www.researchgate.net/publication/362752511_Advances_challenges_and_opportunities_in_creating_data_for_trustworthy_AI.

[22] F. Liu, et al., "Anomaly detection in quasi-periodic time series based on automatic data segmentation and attentional LSTM-CNN," IEEE Transactions on Knowledge and Data Engineering, vol. 34, no. 6, pp. 2626–2640, 2020. [Online]. Available: https://www.researchgate.net/publication/343492730_Anomaly_Detection_in_Quasi-Periodic_Time_Series_based_on_Automatic_Data_Segmentation_and_Attentional_LSTM-CNN.

[23] A. Manoharan and M. Sarker, "Revolutionizing cybersecurity: Unleashing the power of artificial intelligence and machine learning for next-generation threat detection," International Research Journal of Modern Engineering and Technology & Science, 2023. [Online]. Available: https://www.researchgate.net/publication/379308659_REVOLUTIONIZING_CYBERSECURITY_UNLEASHING_THE_POWER_OF_ARTIFICIAL_INTELLIGENCE_AND_MACHINE_LEARNING_FOR_NEXT-_GENERATION_THREAT_DETECTION.

[24] N. S. Musa, et al., "Machine learning and deep learning techniques for distributed denial of service anomaly detection in software-defined networks—current research solutions," IEEE Access, vol. 12, pp. 17982–18011, 2024. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10418146.

[25] D. Nair and N. Mhavan, "Augmenting cybersecurity: A survey of intrusion detection systems in combating zero-day vulnerabilities," in Smart Analytics, Artificial Intelligence and Sustainable Performance Management in a Global Digitalised Economy, Emerald Publishing Limited, 2023. [Online]. Available: https://doi.org/10.1108/S1569-37592023000110A007.

[26] M. Ozkan-Okay, et al., "A comprehensive survey: Evaluating the efficiency of artificial intelligence and machine learning techniques on cybersecurity solutions," IEEE Access, vol. 12, pp. 12229–12256, 2024. [Online]. Available: https://doi.org/10.1109/ACCESS.2024.3355547.

[27] G. Pang, C. Shen, L. Cao, and A. Van Den Hengel, "Deep learning for anomaly detection: A review," ACM Computing Surveys, vol. 54, no. 2, Article 38, 2021. [Online]. Available: https://doi.org/10.1145/3439950.

[28] A. Yaseen, "The role of machine learning in network anomaly detection for cybersecurity," Sage Science Review of Applied Machine Learning, vol. 6, no. 8, pp. 16–34, 2023. [Online]. Available: https://journals.sagescience.org/index.php/ssraml/article/view/126.

[29] Z. Zamanzadeh Darban, et al., "Deep learning for time series anomaly detection: A survey," ACM Computing Surveys, vol. 57, no. 1, pp. 1–42, 2024. [Online]. Available: https://dl.acm.org/doi/10.1145/3691338.

[30] X. X. Zhu, et al., "Deep learning in remote sensing: A comprehensive review and list of resources," IEEE Geoscience and Remote Sensing Magazine, vol. 5, no. 4, pp. 8–36, 2017. [Online]. Available: http://dx.doi.org/10.1109/MGRS.2017.2762307.