10th International Conference on Control Engineering &Information Technology (CEIT-2025)
Proceedings Book Series –PBS- Vol 23, pp.303-313

Recent Trends in AI and ML for Cybersecurity: A Comprehensive Review

Sedieg .A Elatab[1] , Rabee H. Gareeb[2] , Azdihar A. Ahmed[3] , [4]Riyadh A.Alsayih

[1]*College of Technology Engineering Surman, Libya*

[2]*Sabratha University, Economy College, Libya.*

[3]*Sabratha University, Faculty of Engineering, Libya*

[4]*Surman College of Science & Technology*

[1]it2017cisco@gmail.com
[2]rabee@sabu.edu.ly

[3]Ezdihar.alwheshe@sabu.edu.ly

[4]riyad.alsaeh@academy.edu.ly

***Abstract* - This paper provides an overview of the current applications of machine learning (ML) and artificial intelligence (AI) in cybersecurity, highlighting their significant roles in areas such as intrusion detection, network security, and malware detection. However, the paper also addresses the challenges these technologies face, including issues of data privacy, model interpretability, and ethical considerations. A comprehensive literature review from reputable journals reveals substantial research gaps and the need for further investigation into these topics. The findings indicate that while AI and ML hold immense potential for enhancing cybersecurity measures, organizations must also navigate the ethical implications of their deployment. In conclusion, the integration of AI and ML in cybersecurity not only improves detection and response capabilities but also opens new avenues for research and application. It is crucial to adopt a balanced approach that considers both the advantages and ethical concerns associated with these technologies to fully leverage their benefits in safeguarding digital assets.**

***Keywords* - AI; ML; cybersecurity; intrusion detection; malware detection; network security.**

I. INTRODUCTION

Cybersecurity is a crucial issue since different industries are becoming more and more dependent on technology, which has increased cyberthreats. Interest in machine learning (ML) and artificial intelligence (AI) as potential remedies has increased as traditional security techniques are failing to withstand sophisticated attacks [1]. These technologies can detect threats that have not yet been identified and improve cybersecurity systems that are already in place.

This study examines current developments in AI and ML applications in cybersecurity, outlining their functions in network security, malware detection, and intrusion detection. With the goal of supplying researchers and practitioners with insights, it also addresses difficulties and unanswered research questions in the field.

Ransomware and malware attacks have increased, highlighting the pressing need for stronger cybersecurity defenses. Even though AI and ML have a lot of potential for real-time analytics and decision-making, issues with

ISSN: 2961-6611

data privacy and ethical application still exist. The study highlights that effective cybersecurity requires a multifaceted strategy that combines cutting-edge technologies with conventional techniques.

The study is a useful tool for determining areas for improvement and formulating plans to incorporate AI and ML into cybersecurity procedures since it offers a thorough review of these technologies' applications, such as threat intelligence and anomaly detection [2].

A. Motivation

Significant advances in cybersecurity have resulted from the quick development of AI and ML, which need to be understood and kept current. Cybersecurity is now a major concern for both individuals and organizations due to the growing complexity of cyberthreats and the increasing frequency of cyberattacks. This research is essential for protecting digital assets and privacy because AI and machine learning have the potential to improve cybersecurity by offering new ways to identify and counteract cyberthreats. The information in Table I and Fig.1 emphasizes how crucial cybersecurity measures are to defending against the different kinds of cyberattacks. It is crucial to maintain vigilance and put in place efficient security procedures to protect against these attacks, which are becoming more frequent and sophisticated against possible dangers.

TABLE I
PRESENT CYBERATTACK TRENDS

Cyberattack Trends	Number of Attacks	Percentage
Malware attacks	5.6 billion	43%
Encrypted threats	3.8 million	4%
Intrusion attempts	4.8 trillion	20%
Crypto jacking attacks	304.6 million	28%
Ransomware attacks	304.6 million	62%
IoT attacks	56.9 million	66%

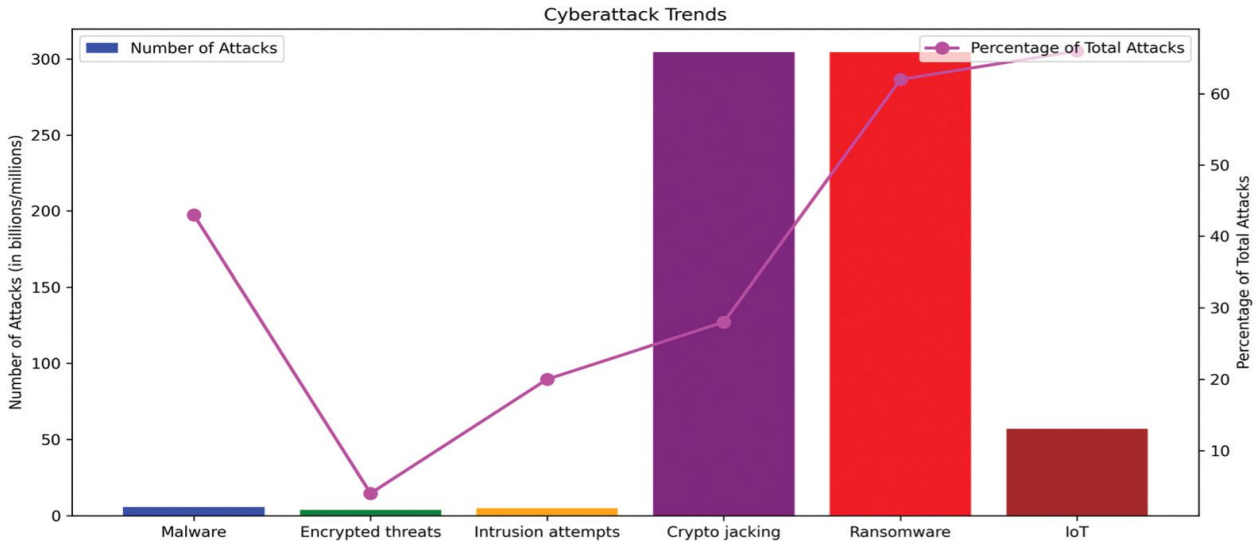

Fig.1 Present Cyberattack trends

ISSN: 2961-6611

II. LITERATURE REVIEW

A. *Overview*

This section of the article explains how AI and ML are revolutionizing cybersecurity, highlighting how they can improve systems and identify new threats. Intrusion detection and response (IDS and IRS) are important applications that use AI and ML to detect threats and adjust to evolving attack patterns through the use of methods like support vector machines, decision trees, and neural networks. Additionally, AI and ML strengthen network security against a variety of cyberthreats, such as Advanced Persistent Threats (APTs) and DDoS attacks, and enhance malware detection [3].
AI and ML technologies can also automate security procedures, monitor network traffic, and identify anomalies. But there are issues with integrating these technologies, like model interpretability, biases, and errors, that must be resolved for efficient application.

B. Intrusion and Response

The substantial influence of machine learning (ML) and artificial intelligence (AI) on cybersecurity is covered in this section, with a focus on how these technologies can improve intrusion detection and response (IDS and IRS) systems. By using methods like decision trees, neural networks, and support vector machines, these technologies assist in identifying threats and adjusting to changing attack patterns. Moreover, AI and ML enhance malware detection and fortify defenses against a range of online dangers, such as Advanced Persistent Threats (APTs) and DDoS attacks. However, a number of obstacles prevent AI and ML from reaching their full potential in cybersecurity. One of the main problems with AI/ML models is that they are not interpretable or explainable, which can make adoption more difficult. Furthermore, biases and inadequate minority class detection may result from training on datasets that are unbalanced, meaning that one class predominates. The efficacy of these systems is further complicated by false alarms, which happen when harmless activities are mistakenly classified as threats [4].

Improving model interpretability, managing unbalanced datasets, and lowering false alarms through increased model accuracy and human expertise are essential to overcoming these obstacles. As indicated in Table II, these problems must be resolved if AI and ML-based IDS and IRS systems are to continue to advance and function effectively in the cybersecurity environment.

TABLE II
AI AND ML TECHNIQUES AND THE CHALLENGES

AI/ML Intrusion Detection Techniques	Advantages	Challenges
Anomaly Detection	Effective for identifying unknown threats	Difficult to differentiate between benign and malicious anomalies
Supervised Learning	High accuracy in detecting known threats	Requires labeled training data.
Unsupervised Learning	Can identify new and unknown threats	Limited interpretability and explain ability.

C. Malware detection

This section emphasizes the significance of malware detection in cybersecurity while highlighting the drawbacks of conventional techniques that depend on pre-established rules and signatures that are simple for attackers to get around. Artificial intelligence (AI) and machine learning (ML) methods, especially deep learning, have been used more and more to enhance malware detection [5]. Highly sophisticated deep learning algorithms, like Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), are trained on extensive datasets to improve their capacity to accurately detect and classify malware. To further enhance training capabilities, generative models such as Variational Auto encoders (VAEs) and Generative Adversarial Networks (GANs) are employed to generate high-quality synthetic data that mimics real-world

ISSN: 2961-6611

patterns. The performance and dependability of malware detection systems have also been shown to be improved by ensemble learning approaches, which integrate the knowledge of several machine learning models [6]. Although there are still obstacles to overcome, the combination of AI and ML has shown encouraging results in this field. The text cites a table that lists popular AI and ML methods and the difficulties they present.

D. Network security and protection tools

To protect computer networks and systems from abuse, disruption, and illegal access, network security is crucial. Artificial intelligence (AI) and machine learning (ML) techniques have been used to detect unknown threats and adapt to changing attack patterns because attackers can evade traditional methods. One popular AI method for network security is behavior-based intrusion detection [7]. These systems analyses and classify network traffic based on its behavior using AI algorithms [8]. The percentage of AI and ML implementation in network security is shown in Fig.2 and Fig.3. PyCharm and Python libraries were used to create all of the research's figures. Table III lists the benefits and drawbacks of AI/ML techniques. These systems have the ability to recognize and categorize anomalies by learning the typical behavior of a network. These irregularities can then be examined in more detail

TABLE III
AI AND ML TECHNIQUES AND THE CHALLENGES

AI/ML Techniques	Advantages	Challenges
Deep Learning	Can identify complex patterns and features.	Requires large amounts of training data.
Ensemble Learning	Combines multiple models for improved performance	Can be computationally expensive.
Behaviour-based Analysis	Can detect unknown malware	Can be difficult to distinguish between benign and malicious behavior.
Natural Language Processing	Can identify obfuscated code	Limited applicability to certain types of malwares.

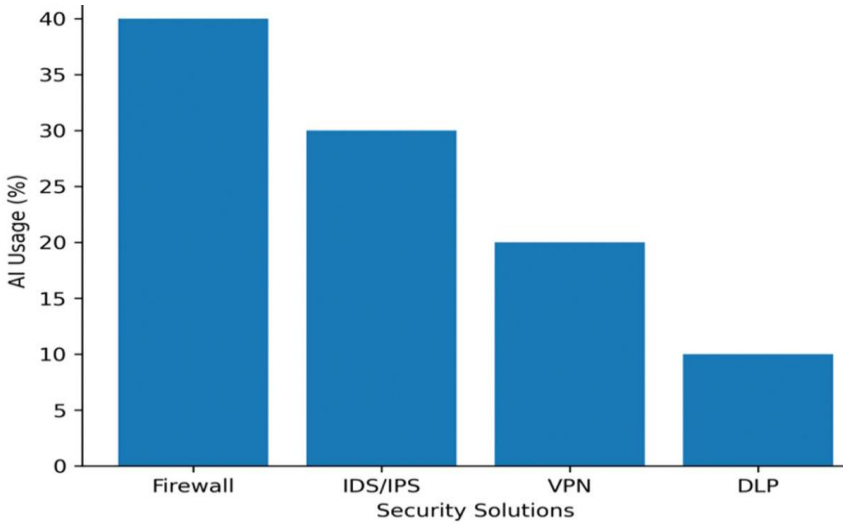

Fig .2 Use AI in network security

ISSN: 2961-6611

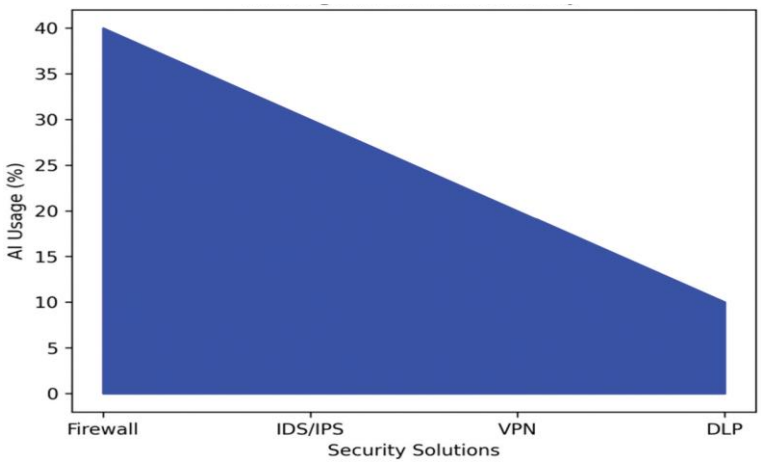

Fig3. Use AI in network security

To detect possible cyberattacks [9], [10]. Unsupervised learning is another well-liked AI technique for network security. To identify patterns in network traffic that differ from typical behavior, unsupervised learning algorithms like clustering and anomaly detection are used. By combining similar network traffic into groups and detecting any traffic that does not fit into a group, these algorithms are able to detect cyberattacks that were previously unknown. Network security also makes extensive use of machine learning techniques, such as reinforcement learning. Network security system behavior is optimized, especially by reinforcement learning algorithms. These algorithms improve the decision-making capabilities of network security systems by learning from the results of their actions through a process of trial and error [11],[12]. The performance of network security systems has been shown to improve with the integration of AI and ML. Nevertheless, there are still issues that need to be resolved, like managing the massive volume of network data, improving the interpretability and explain ability of AI and ML models, and addressing false alarms. To sum up, network security is a crucial component of cybersecurity, and integrating AI and ML into network security systems has demonstrated encouraging outcomes in terms of performance improvement [11],[13]. Table IV lists the benefits and drawbacks of AI/ML techniques.

TABLE IV
AI AND ML TECHNIQUES AND CHALLENGES

AI/ML Techniques	Advantages	Challenges
Behavior-based intrusion detection	Learns normal network behavior to identify and classify anomalies, can identify potential cyber-attacks	Limited accuracy with new and unknown threats
Unsupervised learning	Can identify patterns in network traffic that deviate from normal behavior, can detect previously unknown cyber-attacks	Limited interpretability and explainability
Reinforcement learning	Can optimize behavior of network security systems, improves decision-making	Requires a trial-and-error process for learning
Ensemble learning	Can improve detection system performance by combining multiple models	Requires significant computational resources
Deep learning (e.g. CNN, RNN)	Can identify malware and learn from vast amounts of data	Requires large amounts of data for training, limited interpretability
Generative models (e.g. GANs, VAEs)	Can generate synthetic data for training and improve detection	Limited interpretability and explain ability

ISSN: 2961-6611

III.OVERVIEW OF GENERATIVE AI IN CYBERSECURITY

One of the most significant developments in cybersecurity is artificial intelligence. The ability to proactively identify threat patterns, quickly capture significant risks, and launch self-activated rapid responses to lessen the impact of cyber threats has greatly increased with the advent of Generative Artificial Intelligence (GenAI). However, these technological developments give malicious actors the chance to take advantage of these systems for more harmful ends. In order to improve and fortify offensive and defensive strategies against constantly evolving threats, the cybersecurity sector is placing a high priority on the rapid adoption of GenAI. The anticipated expansion of generative AI in the security market is depicted in Fig.4 [14].

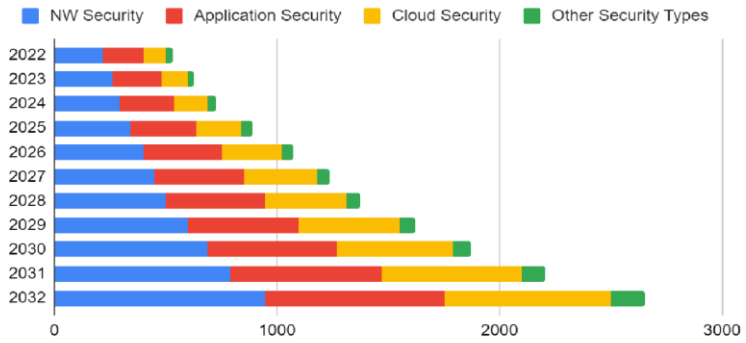

Fig.4 Generative AI in the Security Market 2022-2032 (USA Millions)

Fig.4 presents the estimated growth of GenAI in cybersecurity from 2022 to 2032. It also highlights the major domains where generative AI is most likely to be applied, such as network security, application security, cloud security, and other security domains [14].

IV.AI-BASED APPROCHES IN CYBERSECURITY

Thanks to developments in computing technologies, our society is rapidly evolving and has a big impact on people's daily lives and jobs. Machines that can think, learn, make decisions, and solve problems like humans have been produced by some of these technologies. AI, for instance, is intelligent and capable of making decisions and analysing data in real time while processing massive volumes of information to address issues. AI techniques can be applied to a wide range of scientific and technological domains. It's no secret that there is a wealth of personal data on the Internet, which leads to numerous cybersecurity problems. First, the volume of data makes manual analysis nearly impossible. Second, there may be an increase in threats or threats based on AI. Additionally, the cost of preventing threats rises due to the high cost of hiring specialists. Additionally, developing and implementing algorithms to identify those threats requires a significant investment of time, money, and effort. Using AI-based techniques is one way to address those problems.

AI is capable of quickly, accurately, and efficiently analyzing vast amounts of data. Even if their patterns change, an AI-based system can use threat history to anticipate similar attacks in the future. The following justifies the use of AI in cyberspace [15]: AI is capable of handling large amounts of data, identifying new and significant changes in attacks, and continuously learning to improve security systems' responses to threats.

However, there are some drawbacks to AI as well. For example, an AI-based system needs a lot of data, and processing that massive amount of data takes a lot of time and resources. Additionally, end users may experience false alarms frequently, and efficiency may suffer if necessary responses are delayed. Additionally, adversarial inputs, data poisoning, and model stealing are ways that attackers can target the AI-based system.

Recently, researchers have discovered ways to use AI techniques to identify, thwart, and react to cyberattacks. Four major categories can be used to classify the most prevalent kinds of cyberattacks:

A. Software exploitation and malware identification

- Software exploitation**:** A portion of software vulnerabilities are exploitable, meaning that an attacker with knowledge of the flaw can target the underlying software program. Buffer overflow, integer overflow, SQL injection, cross-site scripting, and

ISSN: 2961-6611

cross-site request forgery are a few common software vulnerabilities. Vulnerabilities are found and fixed. Given the high costs of software development and the pressure to get the product onto the market, it would have been ideal if developers had discovered and addressed every vulnerability during the design and development phase. As a result, issues are constantly identified and fixed. Bruce Schneider asserts that "the internet can be regarded as the most complex machine mankind ever built." We hardly know how it functions, much less how to protect it [16]. It is time-consuming to go through code line by line to fix software bugs, but if computers are taught what the vulnerabilities look like, they can do it. AI seems to be capable of completing these tasks. Benoit Moral [17] explained how AI techniques in particular contribute to increased application security. With a focus on web application security, this study promoted the use of Bayesian algorithms, probabilistic reasoning, and knowledge-based systems to identify software exploitations.

- Malware identification: It is a widely used technique for cyberattacks. Trojan horses, worms, and viruses are examples of malicious software. Preventing and reducing malware attacks is essential because of the significant influence that malware has on politics and the economy. As a result, a lot of research has been done on implementing AI techniques. Here is a list of some noteworthy studies. A framework for categorizing and identifying malware through data mining and machine learning classification was established by the authors in [18]. In order to identify unknown malware, the researchers in [19] employed support vector machines and k-nearest neighbors as machine learning classifiers. To identify intelligent malware, a different method [20] developed a deep learning architecture. Mobile malware was the subject of a recent malware detection study. A deep convolutional neural network was used to detect malware in [21]. In [22], To detect malware, the authors developed a brand-new machine learning algorithm called rotation forest. Using bio-inspired computation to classify malware was another area of study. This method was applied to optimize parameters for classification. The authors of [23],[24] improved malware detection efficiency by utilizing genetic algorithms.

B. Network intrusion detection

- Denial of Service (DoS): This attack, which is one of the most common attacks, occurs when authorized users are unable to access information, devices, or other network resources due to cybercriminals' action. The authors in [25], proposed a system that applies two different approaches, namely, anomaly based distributed artificial neural networks and signature-based approach.
- Intrusion Detection System (IDS): An intrusion detection system (IDS) shields a computer system from anomalous activity, violations, or impending dangers. They are suitable for creating IDS because of their adaptability, speedy computations, and ease of learning AI-based technologies. In order to lower false alarms, AI-based algorithms aim to enhance classifiers and optimize features. To develop a model for IDS, the authors in [26] combined a support vector machine with a modified form of k-means. A fuzziness-based reinforcement learning method for IDS was introduced by the authors in [27]. To improve performance, they employed supervised learning with unlabeled sample datasets. Another method, [28], predicted network traffic for a specified time period using fuzzy logic and genetic algorithms for network intrusion detection.

C. *Phishing and spam detection:*

- Phishing attack: Phishing attacks aim to obtain a user's personal information. Phishing attacks include dictionary attacks and brute-force attacks. Here are a few noteworthy AI-based strategies to address this problem. In [29], the authors presented a phishing email detection system that used reinforcement learning and a modified neural network. Feng et al. used neural networks and the Monte Carlo algorithm and risk minimization strategy in [30] to detect phishing websites.
- Spam detection: This is a reference to unsolicited bulk emails. Unsuitable content in spam emails can cause security problems. Spam emails have recently been filtered using AI-based algorithms. One system, for example, was introduced by Feng et al. [25]. This system filtered spam emails by combining the naive Bayes algorithm with support vector machines.

AI can be used to analyses data for attack detection and response in a variety of cyberspace domains. Security analysts can work more quickly with semi-automated systems to identify cyberattacks because AI can also automate processes. Below are a few well-liked methods for using AI in cybersecurity:

D. *Threat detection and classification:*

AI techniques are able to recognize dangers and stop attacks before they happen. This is typically achieved by developing a model for identifying patterns of malicious activity in large datasets of cybersecurity events. In order to monitor, identify, and react to threats in real time, the model usually consists of recorded Indicators of Compromise (IOC) and historical data surveillance. As a result, the models automatically identify similar activities if they are found. IOC datasets are used by ML classification algorithms to detect and categories the various malware behaviors in datasets [31]. Moreover, behavioral-based analysis examines the behavior of thousands of malwares using machine learning clustering and classification algorithms [32]. Additionally, the patterns can be used to automate the detection process and categorizing emerging dangers. Security

ISSN: 2961-6611

analysts and other automated systems can also gain a lot. For example, machine learning algorithms can automatically recognize similar attacks by using historical datasets that include detailed events of WannaCry ransomware attacks.

E. *Network risk scoring:*
This quantitative metric gives various network segments risk scores. Using this metric, cybersecurity resources are ranked according to risk scores. By examining historical cybersecurity datasets, artificial intelligence (AI) can automate this process and identify network segments that are more susceptible to particular kinds of attacks.

F. *Automated processes and optimize human analysis:*
Repetitive tasks completed by security analysts during security actions can be automated by AI. Analyzing reports on previous actions produced by security analysts to successfully detect and counteract specific attacks is one way to automate the process. Using this information, AI algorithms create a model that can subsequently be used to find related online activity. AI algorithms react to attacks using this model without the need for human inference. Automating the entire security process can be challenging at times. In this instance, AI can be integrated into the cybersecurity workflow, allowing computers and system analysts to collaborate on tasks [33].

V. ETHICAL CONSIDERATIONS OF AI IN CYBERSECURITY

The integration of AI into cybersecurity offers significant benefits but also raises important ethical concerns. Issues such as data privacy, transparency, accountability, and bias must be carefully managed to ensure AI systems are used responsibly and in compliance with legal standards like GDPR. Table V summarizes the key ethical issues associated with the use of AI in cybersecurity. Each issue is paired with its underlying cause and a practical example to illustrate its implications.

Table V. COMMON ETHICAL ISSUES OF AI IN CYBERSECURITY

Ethical Issue	Root Cause / Contributing Factor	Example
Data Privacy and Consent	Use of large-scale personal data from multiple sources without unified or explicit user consent.	A cybersecurity company using user data from social media must ensure it complies with GDPR requirements for explicit consent .
Data Minimization	Over-collection of data driven by the need to improve model performance.	A company aiming to enhance malware detection may collect more user data than necessary, risking GDPR non-compliance.
Algorithmic Bias	Training datasets reflecting societal or demographic imbalances.	A facial recognition system trained mainly on one demographic may perform poorly for others, leading to unfair access control outcomes .
Transparency and Explainability	Use of complex ML models ("black boxes") that make automated decisions difficult to explain.	If a system flags a user as suspicious, GDPR requires an explanation, which may not be possible if the AI model lacks interpretability .
Accountability and Liability	Lack of clarity around who is responsible when AI systems make incorrect or harmful decisions.	When a legitimate user is denied access due to AI misclassification, it raises the question: Is the developer, operator, or AI system at fault? .
Cross-Border Data Transfers	Conflicts between international data regulations and cloud-based cybersecurity operations.	A company using a U.S.-based cloud service must navigate GDPR's strict rules for transferring personal data outside the EU .
Data Breach Notification	Tension between timely disclosure and organizational desire to minimize reputational harm.	GDPR requires breach notifications within 72 hours, but a company might delay disclosure of a sensitive incident to avoid negative publicity, raising ethical concerns .

ISSN: 2961-6611

IV. CONCLUSION

In summary, this paper has explored the transformative impact of machine learning (ML) and artificial intelligence (AI) on the field of cybersecurity, emphasizing their critical roles in enhancing intrusion detection, network security, and malware detection. The integration of these technologies presents significant opportunities for improving organizational defenses against an increasingly complex landscape of cyber threats. However, the study also highlights substantial challenges, including issues related to data privacy, model interpretability, and ethical considerations that must be addressed to ensure responsible deployment.

As organizations increasingly turn to AI and ML solutions, it is vital to navigate the ethical implications of these technologies carefully. Ensuring transparency and fairness in AI algorithms is essential to mitigate biases and enhance trust among users and stakeholders. The literature review indicates that while there has been considerable progress, research gaps remain that require further investigation, particularly in developing trustworthy AI systems that can adapt to the evolving threat landscape.

Looking forward, the future of cybersecurity will likely hinge on the continued development of AI and ML methodologies, coupled with a robust ethical framework that guides their application. This multifaceted approach will not only enhance the effectiveness of cybersecurity measures but also foster a more secure digital environment. By embracing both cutting-edge technologies and traditional security practices, organizations can build resilient defenses capable of withstanding the challenges posed by sophisticated cyber threats. Ultimately, the path forward in cybersecurity will involve a balanced integration of innovation, ethics, and practical application, ensuring that digital assets are safeguarded against current and future risks.

REFRENCES

[1] Bresniker, K., Gavrilovska, A., Holt, J., Milojicic, D., & Tran, T. (2019). Grand challenge: Applying artificial intelligence and machine learning to cybersecurity.
[2] Benzaid, C., & Taleb, T. (2020). AI for beyond 5G networks: A cyber-security defense or offense enabler? *IEEE Network*, *34*(6), 140–147
[3] Pinto, A., Herrera, L. C., Donoso, Y., & Gutierrez, J. A. (2023). Survey on intrusion detection systems based on machine learning techniques for the protection of critical infrastructure. *Sensors*, *23*(5), 2415.
[4] Abiodun, O. I., Jantan, A., Omolara, A. E., Dada, K. V., Mohamed, N. A., & Arshad, H. (2018). State-of-the-art in artificial neural network applications: A survey. *Heliyon*, *4*(11), e00938.
[5] Ryalat, M., ElMoaqet, H., & AlFaouri, M. (2023). Design of a smart factory based on cyber-physical systems and Internet of things towards industry 4.0. *Applied Sciences*, *13*(4), 2156.
[6] Stavropoulos, P., Papacharalampopoulos, A., & Sabatakakis, K. (2023). Robust and secure quality monitoring for welding through platform-as-a-service: A resistance and submerged arc welding study. *Machines*, *11*(2), 298.
[7] Zhang, G., Luo, L., Zhang, L., & Liu, Z. (2023). Research progress of respiratory disease and idiopathic pulmonary fibrosis based on artificial intelligence. *Diagnostics*, *13* (3), 357.
[8] Namiot, D., Ilyushin, E., & Chizhov, I. (2022). Artificial intelligence and cybersecurity. *International Journal of Open Information Technologies*, *10*(9), 135–147.
[9] ElKashlan, M., Elsayed, M. S., Jurcut, A. D., & Azer, M. (2023). A machine learning-based intrusion detection system for IoT Electric Vehicle Charging Stations (EVCSs). *Electronics*, *12*(4), 1044.
[10] Stavropoulos, P., Papacharalampopoulos, A., & Sabatakakis, K. (2023). Robust and secure quality monitoring for welding through platform-as-a-service: A resistance and submerged arc welding study. *Machines*, *11*(2), 298.
[11] Munir, M. S., Dipro, S. H., Hasan, K., Islam, T., & Shetty, S. (2023). Artificial intelligence-enabled exploratory cyber-physical safety analyzer framework for civilian urban air mobility. *Applied Sciences*, *13*(2), 755.
[12] Koryzis, D., Margaris, D., Vassilakis, C., Kotis, K., & Spiliotopoulos, D. (2023). Disruptive technologies for parliaments: A literature review. *Future Internet*, *15* (2), 66.
[13] Werbińska-Wojciechowska, S., & Winiarska, K. (2023). Maintenance performance in the age of industry 4.0: A Bibliometric performance analysis and a systematic literature review. *Sensors*, *23*(3), 1409.
[14] Elatab and Almaktoof, Artificial Intelligence in Cyber Security: A Comprehensive Overview, First International Conference on AI: Current Research, Industry Trends, and Innovations (FICAILY2025), Libya.
[15] Thanh Cong Truong, Quoc Bao Diep, Ivan Zelinka, “Artificial Intelligence in the Cyber Domain: Offence and Defense,”. Symmetry Journal, March 2020.

ISSN: 2961-6611

[16] Manjeet Rege, Raymond Blanch K. Mbah, “Machine Learning for Cyber Defense and Attacks,”. The seventh international conference on data analytics, 2018.
[17] K. Rieck, P. Trinius, C. Willems, and T. Holz, “Automated analysis of malware behavior using machine learning,”. Journal of Computer Security, 2011.
[18] Bruce Schneier, “We Have Root,”. Wiley 2019.
[19] Benoit Morel, “Artificial Intelligence a Key to the Future of Cybersecurity,”. In Proceeding of Conference AISec’11, October 2011, Chicago, Illinois, USA.
[20] Chowdhury, M., Rahman, A., Islam, R., “Malware analysis and detection using data mining and machine learning classification,”. In Proceedings of the International Conference on Applications and Techniques in Cyber Security and Intelligence, Ningbo, China, 16–18 June 2017; pp. 266-274.
[21] H. Hashemi, A. Azmoodeh, A. Hamzeh, S. Hashemi, “Graph embedding as a new approach for unknown malware detection,”. J. Comput. Virol. Hacking Tech. 2017, 13, 153-166.
[22] Y. Ye, L. Chen, S. Hou, W. Hardy, X. Li, “DeepAM: A heterogenous deep learning framework for intelligent malware detection,”. Knowledge Information System. 2018, 54, 265-285.
[23] N. McLaughlin, J. Martinez del Rincon, B. Kang, S.Yerima, P. Miller, S. Sezer, Y. Safaei, E. Trickel, Z. Zhao, A. Doupe, “Deep android malware detection,”. In Proc of the Seventh ACM on Conference on Data and application Security and Privacy, Scottsdale, AZ, USA, 22-24 March 2017, pp.301-308.
[24] H.J. Zhu, Z.H. You, Z.X. Zhu, W.L. Shi, X. Chen, L. Cheng, “Effective and robust detection of android malware using static analysis along with rotation forest model,”. Neurocomputing 2018, 272, 638-646.
[25] F.V. Alejandre, N.C. Cortés, E.A. Anaya, “Feature selection to detect botnets using machine learning algorithms,”. In Proceedings of the 2017 International Conference on Electronics, Communications and Computers (CONIELECOMP), Cholula, Mexico, 22–24 February 2017; pp. 1-7
[26] A. Fatima, R. Maurya, M.K. Dutta, R. Burget, J. Masek, “Android Malware Detection Using Genetic Algorithm based Optimized Feature Selection and Machine Learning,”. In Proceedings of the 2019 42nd International Conference on Telecommunications and Signal Processing (TSP), Budapest, Hungary, 1–3 July 2019; pp. 220-223.
[27] W.L. Al-Yaseen, Z.A. Othman, M.Z.A. Nazri, “Multilevel hybrid support vector machine and extreme learning machine based on modified K-means for intrusion detection system,”. Expert Syst. Appl. 2017, 67, 296-303.
[28] R.A.R. Ashfaq, X.Z. Wang, J.Z. Huang, H. Abbas, Y.L. He, “Fuzziness based semi-supervised learning approach for intrusion detection system,”. Information Science, 2017, 378, 484-497.
[29] A.H. Hamamoto, L.F. Carvalho, L.D.H. Sampaio, T. Abrao, M.L. Proenca, “Network anomaly detection system using genetic algorithm and fuzzy logic,”. Expert System Application. 2018, 92, 390-402.
[30] S. Smadi, N. Aslam, L. Zhang, “Detection of online phishing email using dynamic evolving neural network based on reinforcement learning,”. Decision Support System, 2018, 107, 88-102.
[31] F. Feng, Q. Zhou, Z. Shen, X. Yang, L. Han, J. Wang, “The application of a novel neural network in the detection of phishing websites,” Intelligent Humanizing Computation, 2018, 1-15.
[32] W. Feng, J. Sun, L. Zhang, C. Cao, Q. Yang, “A support vector machine based naive Bayes algorithm for spam filtering,”. In Proceedings of the 2016 IEEE 35th International Performance Computing and Communications Conference (IPCCC), Las Vegas, NV,USA, 9-11 December 2016; pp. 1-8.
[33] Sabah Alzahrani, Liang Hong, “Detection of Distributed Denial of Service (DDoS) attacks Using Artificial Intelligence on Cloud,”. In Proceedings of 2018 IEEE Conference, San Francisco, CA, USA, July 2018.

ISSN: 2961-6611