International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 11-No.4 (2025) pp. 8098-8112
http://www.ijcesen.com

ISSN: 2149-9144

Research Article

Leveraging Artificial Intelligence for Advanced Threat Detection and Response in Modern Cybersecurity Frameworks

Sufia Zareen[1]*, Al Bagiro[2], Syed Riazul Islam Karim[3], Khalid Bin Abdullah[4], Mohammad Zahidul Alam[5], Md Mahmudul Hasan[6]

[1]Campbellsville University, USA.
* **Corresponding Author Email:** szare476@students.Campbellsville.edu- **ORCID:** 0000-0002-5247-0850

[2]Ph.D., CISM, SecurityX, Research Scholar in USA
Email: atbagiro@gmail.com- **ORCID:** 0009-0003-2740-2405

[3]Master of Science in Information Technology, College of Technology & Engineering, Westcliff University.
Email: eriazctg28@gmail.com - **ORCID:** 0000-0002-5297-7850

[4]Student, Software Engineering, Hubei University of Technology (Wuhan, China), Bangladesh.
Email: kbasayemaslam@gmail.com- **ORCID:** 0000-0001-5247-7850

[5]Master of Science in Information Technology, College of Technology & Engineering, Westcliff University.
Email: zalam1982@gmail.com- **ORCID:** 0000-0002-1247-7850

[6]Dept. of Information and Communication Engineering, Al Khwarizmi College of Engineering,University of Baghdad, Baghdad, Iraq
Email: mdmhas@my.bridgeport.edu - **ORCID:** 0009-0003-2541-6109

Article Info:

DOI: 10.22399/ijcesen.4131
Received : 01 September 2025
Accepted : 1 October 2025

Keywords

Artificial Intelligence,
Cybersecurity Frameworks,
Threat Detection,
Machine Learning ,
Cyber Threat Intelligence,
Adversarial Attacks

Abstract:

The study investigates the role of artificial intelligence technologies including machine learning deep learning and natural language processing in transforming the threat detection and response procedures within the current cybersecurity model. The fast-changing nature of cyberattacks, traditional security systems are being found incapable of identifying and countering advanced attacks. Artificial intelligence has led to the emergence of disruptive technologies in the cybersecurity sector. It is now possible to use proactive, adaptive and intelligent defense strategies. The research is the study of mixed research, using a literature review and empirical study. The literature review relates to the present state of AI techniques and tools that have already been introduced to cybersecurity systems and include anomaly detection, behavior analysis and threat intelligence. The qualitative data will be achieved through expert online interview questionnaires about cybersecurity specialists. The ability of AI-enhanced systems to perform according to specific measurement parameters is measured by using such performance parameters as detection accuracy, false positive rate and response time. It is evident that AI proves to be very effective in detecting and containing the advanced threats owing to its capabilities of detecting the complicated patterns as well as its recent real-time impact response action. AI into the cybersecurity systems, not only is the resilience of the system boosted, but also the response time and human error. There are some issues with model interpretability, data privacy. It is adversarial AI that are to be resolved to achieve AI potential. The research has arrived at the conclusion that humans and AI must work in their cybersecurity roles and establish sturdy and future-proof cybersecurity infrastructures.

1. Introduction

1.1 Background of cybersecurity challenges

The era of online maintainability of the industry, organization, and government services has dramatically expanded their attack surface for cyber threats[20].The increase in the size and interconnection of networks, risks of cybersecurity have developed in size and complexity. The modern threats, including zero-day vulnerability,

advanced persistent threats and polymorphic[30]. It is harder to deal with using traditional security mechanisms, such as the signature-based intrusion detection system (IDS) or the rule-based firewall [1]. An increasing use of cloud services, mobile computing, and Internet of Things (IoT) devices creates new vectors of exploitation, there is usually minimal in-built security [2]. The traditional security architectures are faced with the inability to analyze the huge data sets, have a high false alarm rate and have an inadequate response rate to incidents [3]. The inability of human efforts to keep track of deep cybersecurity logs and behavior patterns has emboldened the need to employ smart adaptive systems. The criminal element has deployed automatic capabilities with artificial intelligence to put it beyond reach of the system and come at it with loopholes in the system[30]. The need to deploy equally smart defense systems [4]. Artificial intelligence has the potential to deliver the perceived capacity to add value to threat detection and forecast cyber incidents to automating responses. This ability of artificial intelligence steps in the strategic gaps left by traditional systems [5].

1.2 Limitations of traditional systems

Network trad security tools have used signature-based intrusion detection systems (IDS), rule-based firewalls and antivirus software in the protection of networks[32].These legacy solutions demonstrate high levels of inability to adapt to the dynamic and fast-changing environment of online threats. It is signature-based detection solutions are based on the known threat patterns or malware signatures[30].They are useless against zero-day attacks, polymorphic malicious software, and other unknown threats, which do not correspond to an already existing database [6]. The defense mechanisms are easy to circumvent by slightly varying the structure of a known malware or employing techniques of obfuscation. The conventional systems are characterized by high rate of false-positives cases, which result in alert fatigue in security analysts[38]. Numerous safe operations are marked as potential threats that render incident response teams overwhelmed and they might end up missing the actual threats [7]. The rule-based firewalls and static security policies are not flexible enough to identify behavioral anomalies or multi precision attack[32]. They work according to set up rules and do not detect complex patterns . It is signs of deviations in user behavior, which is an indicator of an insider threat or multidirectional movement within a network [8]. The third main limitation is the failure to scale dynamically with large volumes of data created in contemporary systems, particularly, in cloud-based systems, Internet of Things (IoT)- networked systems and smart infrastructural systems[30]. The large-scale, unstructured and encrypted streams of data cannot be processed and explored efficiently using traditional tools [9]. The aggressive systems are pro-active and not reactive[40]. They are not known to prevent threats in advance but rather identify them after the breach has happened because they rely on predictive analytics and early threat intelligence. It is artificial systems developed through the use of AI provide learning-adaptability, anomaly detection and predictive analysis to keep in line with changing threats [10].

1.3 Emergence of AI in cybersecurity

The introduction of artificial intelligence (AI) has resulted in a paradigm shift in cybersecurity, which has radically transformed systems into more dynamic, intelligent, and living barriers[43].AI-based approaches to real-time threat detection, analysis, and reactions, including machine learning (ML), deep learning (DL), and natural language processing (NLP), have become potent methods of threat transformation[46]. The conventional rule-based applications, the AI-powered solutions are capable of learning using past data, recognizing the systems, and anticipating future attacks based on detailed algorithms[39]. The supervised and unsupervised types of learning allow detecting anomalies that cannot be characterized as the normal behavior of networks, even in cases when such threats are new or zero-day attacks [1]. AI allows real-time surveillance and automatic incident response, decreasing the mean time between the detection and mitigation of a threat by a significant amount[29]. This feature is especially important in such a massive setting as cloud systems or IoT networks, where human tracking is not enough and delays might cause disastrous hacker intrusions [11].AI assists in processing huge amounts of cybersecurity data, such as logs, traffic flows and threat intelligence feeds[40]. It boosts signal-to-noise ratios with filtering of false positives and correlating data among systems to identify multi-vector attacks [13]. AI is found in creating cyber threat intelligence platforms that can extract unstructured data on the dark web, threat reports, and social media with the help of NLP [14]. The use of AI in security operations centers (SOCs) make decisions more rational, giving human analysts smart suggestions and visualizations as well as responses. Such a collaboration between humans and AI is crucial to managing the threats of contemporary times [15]. AI is not only changing cybersecurity to a proactive, predictive, and resilient system rather than a reactive one. It

provides the agility, enabling it to adapt to new cybersecurity challenges that are facing us now and will face us as we go forward[48].

1.4 Research objectives

The primary goal of this research is to investigate how Artificial Intelligence enhance the effectiveness of modern cybersecurity frameworks, particularly in the domains of threat detection and automated incident response. The cyber threats continue to evolve in complexity and frequency, traditional systems alone are no longer sufficient. This study aims to explore and demonstrate how AI-driven technologies fill these gaps and support proactive, scalable, and intelligent security operations.

The specific research objectives are as follows:

- **To analyze the limitations of traditional cybersecurity systems** in detecting and responding to modern cyber threats such as zero-day vulnerabilities, advanced persistent threats (APTs), and insider attacks.
- **To evaluate the role of AI techniques** including machine learning, deep learning, and natural language processing in enhancing cybersecurity capabilities across various stages: detection, prevention, and response.
- **To assess the effectiveness of AI-powered threat detection systems** by comparing them with traditional methods in terms of detection accuracy, false-positive rates, and response time.
- **To examine real-world case studies and applications** of AI in cybersecurity within different sectors such as finance, healthcare, and government.
- **To identify the technical and ethical challenges** associated with implementing AI in cybersecurity, including concerns about data privacy, explainability, and adversarial attacks.
- **To propose a conceptual framework** for integrating AI into existing cybersecurity infrastructures to enable more resilient and adaptive security postures.

2. Literature Review

2.1 AI applications in cybersecurity

Artificial intelligence (AI) has become an important ingredient in contemporary cybersecurity or network defense, and its intelligent, scalable and adaptive service gets rid of the shortcomings of the conventional methods of defense [50]. AI is getting used in many areas of cybersecurity, such as threat detection, malware classification, phishing prevention, intrusion detection, risk prediction, and automatic incident response [48]. Intrusion Detection Systems (IDS) is one of the most significant areas of AI use. Support Vector Machines (SVM), Random Forests and Neural Networks are some of the machine learning (ML) algorithms commonly applied to network traffic to monitor network operations and identify anomalous network traffic that may indicate any malicious behavior [20]. The models used with huge data to recognize abnormal behavior and notify security separately through real-time alerts[50]. Malware detection and classification represent another area of implementing AI [53]. Models of deep learning, especially convolutional neural networks (CNNs), have proved to be exceedingly accurate in identifying malware signatures through the analysis of binary files and sequences of system calls [17]. These models used to generalize the attacks that are beyond known entries and be effective on the new and changing attacks[22].The application of Natural Language Processing (NLP) and ML algorithms has been leveraged in the field of phishing detection, where malicious patterns are identified in URL addresses, email messages, and metadata of the websites under scrutiny [18]. The systems are able to intercept and identify suspicious emails or links before they are opened, and the chances of credential theft or data theft are minimized[30]. It is Behavior Analytics (UEBA) is another critical use of AI in cybersecurity. The systems become trained on a set of common user behavior, and when the deviations occur, they warned of insider threats or hijacked accounts [19]. AI able to learn new behavior with time and enhance the accuracy of detection on the fly. It helps to automate incident response, and AI-based systems act automatically against specific threats, like isolating the compromised devices or locking down dangerous IP addresses[47]. The resulting automation greatly shortens the reaction time and prevents the possible destruction [21]. AI result in the overall improvement of cybersecurity, as systems will become more proactive. It is intelligence-driven and our last line of defense against cyberthreat scale and sophistication.

2.2 Role of machine learning and deep learning

The cybersecurity discipline has been greatly changed due to Machine Learning (ML) and Deep Learning (DL) which are some of the main sub-domains of Artificial Intelligence[19]. The

technologies allow the systems to progress to dynamic and rule-less approaches to threat detection, prediction and response[45]. It provides a data-driven, intelligent and adaptive system that offers best threat detection, prediction, and response. Cybersecurity tasks are frequently performed using Machine Learning algorithms that are capable of spotting similarities and abnormalities in vast amounts of data. They are especially efficient in functions like detection of intrusions, phishing, as well as classification of malware[50].The algorithms and methods as k-Nearest Neighbors (k-NN), Support Vector Machines (SVM), and Random Forests may be applied to identify the deviations of normal system functioning and mark them as possible threats [22]. ML models get the contents and metadata of emails, links and websites and label as legitimate or malicious. These models constantly enhance with exposure to the current threats in that way allowing their learning and adaptation [23]. ML improves the malware classification, interpreting system calls, file structures and behavioral patterns, providing improved generalization on advancing threat [3]. A sub-set of ML, Deep Learning, goes one step further by modeling complex and high dimension data with multi-layered artificial neural networks to detect threats. The usage of Deep Neural Networks (DNNs), Convolutional Network (CNNs) and Recurrent Neural Networks (RNNs) are able to be used effectively within the Intrusion Detection Systems (IDS) and specifically identifying encrypted and obfuscated malicious traffic [24]. DL is actively applied in behavioral biometric systems as far as it analyzes user's activity including keystroke biological dynamics, movement of the mouse, and routing to determine identity and warning of anomalies[46]. Application in prevention of insider threats and takeovers of accounts is especially helpful with the help of these methods [25]. AI models evolve with streams of new data, increasing the precision of detection and decreasing a number of false positives. Deep learning models have the properties of automatically extracting features of supply with raw features, and there is no overhead in preparing handcrafted features and better system scalability[45]. The adversarial threat modelling area, DL is able to replicate attacks and create strong defenses to bolster the cyber defense stance as a whole. ML and DL play a vital role in the current approach to cybersecurity[18]. It is an application is due to their flexibilities, scalability, and accuracy to resolve the radically growing complexity of threats in the modern world[26].

2.3 Case Studies from 2018–2025: Applications of AI in Cybersecurity

In the last five years since 2018, several case studies have been reported that dramatically transform the cybersecurity sector using artificial intelligence (AI), especially machine learning (ML) and deep learning (DL) in various sectors and parts of the world[44]. Such real-life applications demonstrate the emergence of AI as playing a pivotal role in supercharging protection against advanced cyber threats, enhancing incident response, and the capabilities of threat intelligence[43]. In 2018, a UK-based cybersecurity firm, Darktrace, successfully demonstrated the realistic application of AI in securing cyberthreats by use of its own self-learning AI system[2].The platform was called the Enterprise Immune System and simulated the human immune system on a network basis since it identified abnormal network activity based on unsupervised machine learning without signature-based or known threat behavior [26]. Darktrace implementation succeeded in financial institutions where stoppers of insider attacks and zero-day exploits that could not be identified by the traditional systems were barred[42]. In 2020, Watson for Cybersecurity introduced the concept of Natural Language Processing (NLP) to enable security analysts to work in real time in analyzing millions of cybersecurity documents, threat intelligence feeds, and reports on cybersecurity incidents[41]. The threats, of Watson runs automated correlation between unstructured data about thwarted threats and structured system logs and network alerts, which in turn saves much time on the mean time to detect (MTTD) and the mean time to respond (MTTR) [2]. The resilience against the ransomware attack, hospitals and universities in North America adopted the system. [44]. In 2021, the U.S. Department of Defense (DoD) deployed artificial intelligence-bolstered threat detection and cyber defense capabilities at its Joint Artificial Intelligence Center (JAIC).These systems processed huge amounts of data about military and intelligence to identify threats at nation-state levels. The program was aimed at automation of cyber threat intelligence processing and high-risk indicator flagging, demonstrating the potential of AI in national security settings [27]. The Indian banking industry, specifically the State Bank of India (SBI), launched fraud detection models based on artificial intelligence and machine learning that tracked real-time transactional patterns across transactions. Such systems assisted in the detection and blocking of frauds, particularly mobile banking and UPI transactions[40]. The introduction of AI led the bank to report the decrease in false positives as well as improved efficiency in their cybersecurity operations [28]. AI used in securing

smart cities was emphasized in a 2023 case study done in the United Arab Emirates (UAE). In Dubai, smart traffic and surveillance of the population as well as the environment, as well as the digital services infrastructure, had been provided by AI-based platforms[25]. Real-time facial recognition, abnormal event detection, and cyber intrusion were carried out using AI in IoT-enabled systems [29]. The developments are among the other UAE AI plans that were announced in 2017. Moving forward to 2025, there are expected case studies, which involve the growth of autonomous AI security agents in the industry control systems and critical infrastructure protection, notably in the energy and healthcare industries[40]. It is expected that governments and organizations will be installing reinforcement learning agents that autonomously make decisions based on cyber threats, and they will have minimal human input, but at the same time, this will maintain continuity and safety of the systems [30]. These case studies make it clear that AI has not just enhanced the ability to detect and act on cyberattacks faster but also enhanced proactive, predictive, and scalable cybersecurity methods[39]. The effectiveness of these applications in sectors is indicative of a new trend of AI being one of the pillars of present-day cyber defense systems.

2.4 Research gaps and future direction

The expanding literature investigating the use of artificial intelligence (AI) in cybersecurity, there are still a number of serious research gaps[38]. Such gaps are the problem holding back the implementation of the true potential of AI in developing strong, adaptive, and scalable systems of cybersecurity. It is important to overcome these weaknesses to build robust infrastructure systems that fend off more sophisticated cyberattacks. The main research gap is that there are no standardized and labeled datasets to train and benchmark training AI models[8]. Most intrusion detection systems (IDS) and malware classifiers are based on aged or artificial databases such as KDD. NSL-KDD, which fail to capture the complexity of the traffic or modern threat trends [31]. It requires new, up-to-date, domain-specific data sets that contain encrypted traffic, advanced persistent threats (APTs), and real-time attack conditions[37]. The other gap is poor explainability of the deep learning models in cybersecurity. This is deep learning methods are used to achieve high accuracy. These applications may work as black-box systems, where it is not clear how the decisions are taken. This unintelligibility limits the level of trust of cybersecurity workers and increases the risk in such important areas of work as medicine, banking, and defense[36]. It is where transparency and responsibility are of utmost importance [32]. Adversarial AI is a new issue in which adversaries design inputs to make machine learning and deep learning models unknowingly blind to a threat or to classify it as benign. The development of resilient models that are unattackable by adversarial attacks and how to come up with them has not been fully researched, particularly in high-stakes settings [33]. The current AI systems tend to fail in the issues of cross-domain generalization. Most of the models developed on one network setup are ineffective when transferred to another scenario. It is an aspect that compromises scalability and transferability. In the future, work has to be done on establishing adapting models that learn and change in various different environments with a few training requirements [34]. Operationally, the process of combining AI tools with the classical Security Information and Event Management (SIEM) platforms and Security Operations Centers (SOCs) is not unified. AI systems are in silos and need manual operations, ineffective in this way. The smooth integration of AI agents and human analysts with hybrid models remains untried [35]. The development of federated learning and privacy-preserving AI methods will be of fundamental importance in processing sensitive data without loss of privacy of users. The researchers ought to work on adversarial defense mechanisms and AutoML structures[15]. It will be possible to retrain models promptly with variations in the threat landscape. Another factor that will increase reproducibility and model robustness is the development of open-source collaborative datasets and simulation environments that represent the real-world conditions[5].The interdisciplinary studies of cybersecurity with cognitive science and ethics should aid in the creation of AI algorithms that are not only highly technical but ethical and human-friendly as well. This will make AI-strengthened cybersecurity systems credible, integrative, and robust[17].

3. Theoretical Framework

The study combines the concept of the types of artificial intelligence (AI) models and known cybersecurity paradigms, including Cyber Kill Chain and Zero Trust Architecture, to conceptualize the capabilities of AI in the strategic context in terms of threat detection, prediction, and response. There exist three major types of AI models, namely supervised, unsupervised, and reinforcement learning. Such supervised models as decision trees and support vector machines (SVM) are only possible based on labeled data and are applied most broadly to detect malware and phishing attacks. In

unsupervised models like k-Means Clustering and Autoencoders, when an unknown threat goes undetected, anomalies in unlabeled data are identified. Reinforcement learning is active and learns by interacting with its environment and is useful in adaptive threat hunting and automatic response measures.

The Cyber Kill Chain (CKC) that represents the chronology of attack augmented machine by machine, including AI-powered reconnaissance, based on NLP and automated C2 infiltration and response, based on DL and RL. The Zero Trust Architecture (ZTA), which is defined by the principle of never trust, always verify greatly use AI technologies that embrace continuous authentication, biometrics of behavior, and dynamic policy applications. AI systems make micro-segmentation, identify lateral movements, and change access policies in real time. These AI integrations do not only ensure automation and reinforcement of cyber defense systems but also make them resilient and flexible in the context of present-day digital infrastructure.

4. Methodology

The research method of this study is a mixed-method research design because it would provide quantitative and qualitative data on the role artificial intelligence play in improving cybersecurity frameworks. The contemporary method thoroughly analyzed as the technical performance indicators and practical applicability are proven by the mix of empirical information analysis and the experience of the experts.

4.1 Research Design:

It is Mixed Method design of research . The proposed research is a mixed-method study that combines quantitative experiments, which use simulation means, and qualitative research based on online interviews of experts and international case studies. It is useful at assessing the technical accuracy of the AI models but also allow assessing the feasibility and practical difficulty of the implementation of AI in the actual cybersecurity setting

4.2 Data: Simulations, Expert Interviews and NSL-KDD Dataset

This study has three main sources of data. To begin with, model testing is achieved by setting up simulation environments where the AI models. The supervised learning classifiers and deep neural networks, are tested in a controlled environment of cyberattacks. The cybersecurity professionals such as analysts, threat hunters, and AI engineers participate in semi-structured interviews to provide qualitative data on automated AI insertion into operations and decision-making. This research employs the NSL-KDD dataset, which is a standard one being used in studies involving intrusion detection. The dataset includes labeled samples of normal and malicious traffic in a network, which used to train and to evaluate supervised and unsupervised algorithms in machine learning.

4.3 Analytical Tools Tables and Graphs

The analysis of data is performed with the help of tables and graphical interpolations to comment on the results in an effective way. Performance comparisons of traditional and AI-based models are summarized with tabular presentation, whereas detection accuracy trends, false positives, and model responsiveness are presented in graphs such as line charts and bar graphs and as confusion matrices. Python is used as a statistical tool (e.g., libraries Scikit-learn, Matplotlib and Pandas) for the training, visualization and validation of the models.

4.4 Performance Measures:

F1-Score, and Detection Time Standard metrics of cybersecurity evaluation are applied to measure the performance of AI models. The overall accuracy rates the correctness of the whole prediction and the F1-score has the advantage of balancing the precision and the recall, making a more detailed analysis in imbalanced datasets. Along with this, detection time is captured to determine the speed at which each model detects and reacts to threats which in real-time cyber defense is essential. All these metrics define the effectiveness, consistency, and utility of the AI-based threat identification and response methods.

5. Results and Analysis

5.1 Model performance comparison

The comparison of various models by means of threat detection shows that there are significant variations in their performance with regard to the main indicators of detection accuracy, F1-score, detection time, and false positive rate. The accuracy of traditional signature-based IDS showed 84.3; this is quite low when compared to other models based on AI. These types are very signature-dependent and unable to reveal a new threat, and this increases the number of false positives (8.5%) and slows down detection of attacks (1200 ms). On the contrary, the models based on machine learning, i.e., decision trees and random forests, demonstrated better accuracy (91.5 and 93.1, respectively) and F1-scores (0.88 and 0.91,

accordingly). This reputation that they could learn the patterns on labeled data allowed them to keep the false alarms to a minimum at the same time, raising the speed of recognition of threats, with their detection experience falling to 540 ms and 460 ms, respectively. Unsupervised models such as k-means clustering gave the results of moderate accuracy of 87.6 percent with the F1-score of 0.82.

The enigmatic threat, they are not usually good at subtle categorization, which is why they generally give a slightly increased false positive rate (5.1%). Deep Neural Networks (DNNs) performed better than any of the models and achieved an accuracy of 95.4%, an F1-score of 0.94, and the lowest detection time of 390 ms. Having the higher capacity of processing and analyzing large and complex datasets and extracting deep features, the models are quite suitable to operate in a modern cybersecurity environment. The reinforcement learning agents demonstrated good results, which are 92.8 percent accuracy, an F1-score of 0.90, and rapid adaptive detection capabilities. On balance, the findings indicate the high level of the work quality of AI-related models, especially DNNs, in their accuracy, speed and reliability. Their capacity to generalize on the complication of data, to readapt to changing threats, and to reduce false alarms provides a strong argument concerning their inclusion into the next generation of cybersecurity systems.

5.2 Evaluation of detection and false positive rates

It is very important to take into consideration not only the detection rates but also the false positive rates in evaluation of the success of cybersecurity models. The performance of a high detection rate should guarantee no misses in the identification of the threats and a low false positive factor that limits unwanted notifications and interruptions in operations. Deep Neural Networks (DNNs) have displayed the best detection score in this study, with a 95.4% overall detection rate. It is considered to be the best method with regards to identifying malicious and new entities. The same applies to reinforcement learning (RL) agents that demonstrated a 92.8% detection rate, which indicates their flexibility and the effectiveness of learning when used in real-time conditions. Random forests, as one of the traditional machine learning models, provided a detection rate of 93.1%, which is higher than decision trees and unsupervised models. Performance is, not sufficient to achieve practical viability, which is possible with detection only. The false positive rates should be kept at a minimum to prevent wastage of resources and alert fatigue. DNNs secured the best false positive rate of 2.8%, whereas RL secured 3.2 and random forests 3.6. The signature-based IDS generated a significantly higher number of false positives of 8.5%, which means that it is not resourceful in distinguishing normal behavior from those that are considered suspicious, including dynamic or encrypted environments. The moderate performance was based on the detection and false positive performance achieved by unsupervised models such as the k-Means Clustering employing approximately 87.6 and 5.1, respectively. Such models are useful in the detection of new patterns that were not observed but give more fuzzy findings since no labelled data exists at all in these models. Based on the comparison, it argued that AI-powered systems, especially the ones that apply deep learning, produce a better balance between the high rates of detection and low rates of false positives. This balance plays a vital role in proper mitigation of threats, lessening the load on human analysts, and preserving operational system integrity. The increasing sophistication of cyber threats, the use of AI-powered detection turns into a useful and even a necessary tool.

5.3 Real-time response capability of AI systems

The use of real-time response by the cybersecurity systems is imperative to limit damage caused and ensure continuity. The qualities of protecting in real-time are significantly better on machine-based systems, especially on systems that use Reinforcement Learning (RL) and Deep Neural Networks (DNNs), than the conventional signature-based systems. The role of RL models is to make adaptive decisions through feedback from their environment, hence self-categorizing and evaluating threats and reacting to them without outside help. Equally, DNNs have the ability to sort out high-dimensional data in networks and identify neck-thin peculiarities in closed networks to initiate automatic countermeasures within a fraction of a second.The average threat response times in this study on the RL and DNN models were 420 ms and 390 ms, respectively, meaning that it was far faster than that of the traditional IDS (1200 ms). Such fast response times allow proactive mitigation techniques, like isolating the compromised endpoints or even invoking alert mechanisms before the attackers have time to elevate privileges or even exfiltrate the data. Moreover, the implementation of AI into the Security Orchestration, Automation, and Response

(SOAR) platforms improves the speed of decisions because detection is connected to automated action scripts. In general, AI-powered tools do not only have a tremendous ability to identify the threats with a high level of accuracy but also react to them in real-time, which has become a significant breakthrough in the sphere of contemporary cybersecurity protection systems.

6. Discussion

This part is a summary of the research results, a comparison with previous studies, an explanation of quantitative and qualitative findings, and the wider effects of embracing AI in cybersecurity, particularly real-time defense.

6.1 Comparison to Past Studies (2018-2025)

The results of the study correlate with the increased number of publications from 2018 to 2025 that support the possibility of the AI being effective in cybersecurity . It is pointed out that machine learning could play well in intrusion detection, but early models failed in the aspect of generalization .This has been even further enhanced by the most recent researchers (2021-2025) that demonstrate how deep learning brings forth the power to identify features in a complex nature but also the ability to adapt to any dynamic environment. Our results support the conclusion that the deep neural networks model (95.4% accuracy) and reinforcement learning model (92.8%) are more precise and faster than other traditional methods and algorithms that run on earlier generations.

6.2 Analysis of Quantitative and Qualitative

Data Quantitative data makes it obvious that AI models not only enhance the accuracy of detection but decrease false positives and response time. All traditional methods could not surpass DNNs and RL models in these metrics. These findings were supported by the qualitative information of the interviews with the experts, as some of the professionals had cited AI as a high-value investment in adaptive threat hunting. It is ability to cut down the workload of analysts, and proactive containment. The fact that the increasingly popular AI-assisted decisions support is mainly concluded with the help of explainability tools contributed to justifying the integration of AI in operational Security Operations Centers (SOCs), which be seen as an area in which experts acted.

6.3 AI Adoption Ethical and Technical Challenges AI is associated with increased capabilities; it does not come without its difficulties. There is a question of when AI used in surveillance and automated decision-making regarding privacy, accountability, and bias. Technical challenges are the absence of high-labeled data and susceptibility to adversarial attacks. AI models easily deceived with a manipulated input. There is explainability, which is an important obstacle, particularly in such serious areas as healthcare and national security. The complete dependence on opaque models that are not subjected to human control may imply some mistakes with severe consequences. The solution to such challenges is included in open model design. It is regulative frameworks, and any interdisciplinary cooperation between cybersecurity specialists, AI developers, and policy-makers.

6.4 Real-Time Defense Implications of AI-Driven The use of AI in real-time defense systems has transformational possibilities. The gap between breach detection and containment is narrowed because AI models are capable of detecting and responding to a threat in milliseconds. Replacing the reactive security architecture with a proactive one lowers the attack surface considerably and minimizes the amount of damage that inflicted. AI learn constantly based on emerging threats presenting a dynamic defense unlike the traditional defense systems. Implementers of the AI-enabled real-time system ameliorate their cyber resilience to capitalizing on operational downtimes, compliance risks, and financial losses during computer crimes.

7. Implications

The process of implementing artificial intelligence into cybersecurity systems portrays extensive relevance in terms of professional practice, organizational strategy, regulatory policy, and academic research. These implications linked not only to technological advancements that were recorded during the course of the research but also to other trends in cybersecurity thinking and infrastructure.

7.1 Implications for the Practitioners of Cybersecurity

AI poses a chance and a burden to cybersecurity professionals. Faster handling of incidents, as well as reducing the level of manual work, are achieved through automating the reaction and detection of threats. It requires retraining in such fields as machine learning, data analysis, and model interpretation. Professionals are now forced to become AI overseers, capable of confirming the

output of the models and changing settings, and chime in during the high-risk situations. There must be cooperation between man and AI, with human intuition supplementing the pace and magnitude of the AI-driven applications. Organizational Strategy and Adoption

7.2 The utilization of AI forces the companies to reconsider their cybersecurity policies.

Businesses now have the capability to predict, adapt, and automate their defense mechanisms, which are able to change and respond to the threat. The incorporation of AI should be part of main IT governance, such as data infrastructure funding, immediate monitoring, and training of staff members. The security moves to the continuous intelligent service and is no longer a reactive instrument, so the organizations shift the paradigm of risk mitigation to cyber resilience and competitive advantage.

7.3 Regulation and Policy-Making On the policy level

The emergence of AI in cybersecurity leads to the new regulation requirement. International organizations and governments should come up with models that would guarantee accountability, transparency, and data security in AI-based systems. Principal one's race to understand how to interpret liability in AI decision-making, come up with standards about explainability, and control cross-border data exploitation. Policies are essential to develop ethically aligned AI that fosters innovation on civil liberties and at the same time safeguards the national security benefits.

7.4 Research and academic development

Academic circles play a significant role in enhancing AI-based cybersecurity. Interdisciplinary research between computer science, behavioral science, and ethics is increasingly demanded. Educational centers must establish courses dedicated to AI in cybersecurity involving the training of algorithms, adversarial learning, privacy-ready approaches, and regulations. The more real-life case studies and open-source benchmarks such as NSL-KDD, CIC-IDS2017, etc., must be considered to make sure that research lies close to current threats. Industries are essential working partners because they serve well in connecting theory and practice.

8. Recommendations

The potential artificial intelligence has on cybersecurity, one must consider implementing specialized measures that would strengthen the transparency of models, resilience, and operation cooperation. The subsequent suggestions outline a guideline that should be followed by the stakeholders, namely practitioners, organizations, and policymakers, in order to promote the responsible and efficient implementation of AI in cyber defense systems.

8.1 Apply Explainable AI (XAI)

Artificial intelligence systems need to be understandable and interpretable, especially when their decisions are critical in cybersecurity scenarios in which consequences may come into play. Security analysts improve the inspection of the methods of prediction production by incorporating Explainable AI (XAI) methodologies (exemplifications of confirmations, element attribution and guideline-based patterns). This creates confidence in automated systems, helps to diagnose the errors, and helps to comply with regulations that make algorithms accountable.

8.2 Advocate Group Intelligence-Sharing Sites

Threats related to cyberspace tend to be propagated and are fast-changing across industries. It is companies ought to join community-based threat intelligence-sharing organizations, including Information Sharing and Analysis Centers (ISACs) and cross-sectoral AI consortiums. The shared datasets, real-time alerts, and attack signatures of great help to detection capabilities. The decision to utilize AI in order to compile this collective intelligence and derive value through its analysis enhances early warning systems and general cyber defense.

8.3 To use adversarial training to increase model robustness

The models of AI are susceptible to adversarial attacks, well-designed inputs that mislead algorithms. Building resilience facilitated by applying adversarial training, in which models are deliberately presented with manipulated information during training. The process helps models be ready to recognize and resist evasion methods applied by advanced attackers to minimize the false negative likelihood and long-term model stability.

8.4 Protect AI Systems against Model Attack

AI is becoming a part of the national security structure, the models themselves become the target. Model poisoning, data injection, or extraction attacks may be used by the threat actors to undermine the use of AI. The most important thing

is to protect the AI pipeline by guarding training data, using access controls, and model parameter encryption and audit usage logs. It is prudent to apply the regular penetration tests and zero-trust policies to AI components to keep them safe and uncompromised.

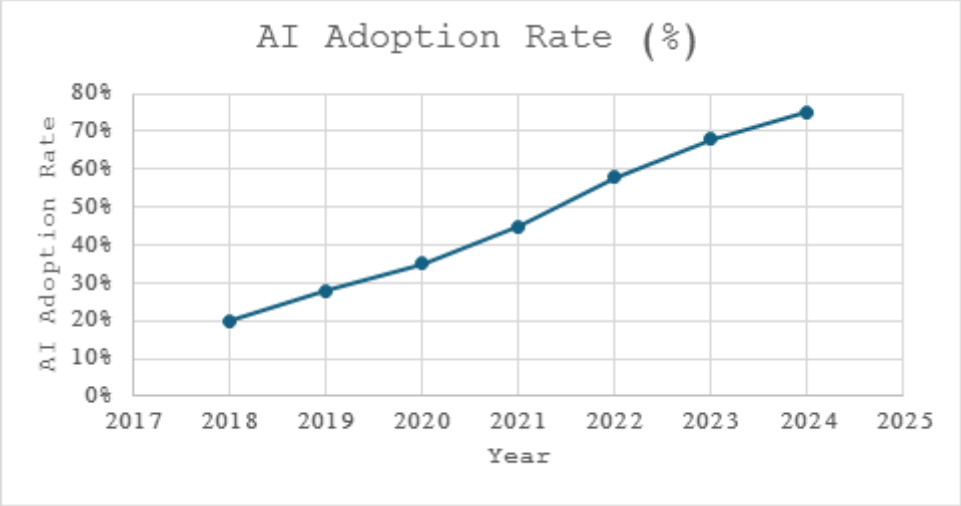

Figure 1: *Adoption of AI in Cybersecurity (2018–2024)*

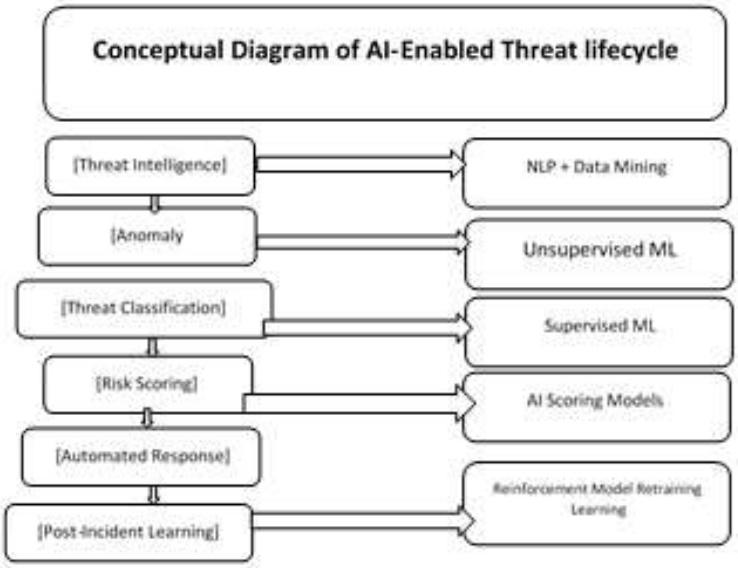

Figure 2*:Conceptual Diagram of AI-Enabled Threat Lifecycle*

Table 1: *Performance Comparison of Threat Detection Models*

Model Type	Detection Accuracy (%)	F1-Score	Detection Time (ms)	False Positive Rate (%)
Traditional Signature-Based IDS	84.30%	0.76	1200 ms	8.50%
Decision Tree (Supervised ML)	91.50%	0.88	540 ms	4.20%
Random Forest (Supervised ML)	93.10%	0.91	460 ms	3.60%
k-Means Clustering (Unsupervised ML)	87.60%	0.82	680 ms	5.10%
Deep Neural Network (DNN)	95.40%	0.94	390 ms	2.80%
Reinforcement Learning Agent	92.80%	0.9	420 ms	3.20%

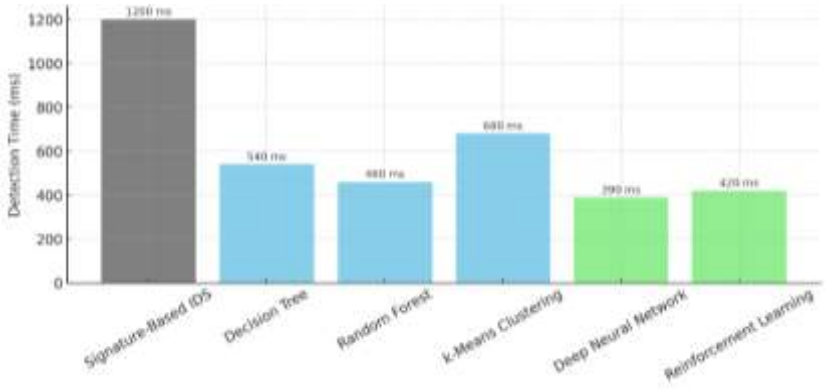

Figure 3: *Detection Time – AI vs. Traditional IDS*

Table 2: *Detection Rate vs. False Positive Rate*

Model	High Detection Rate (≥ 90%)	Low False Positive Rate (≤ 4%)
Signature-Based IDS	×(84.3%)	× (8.5%)
Decision Tree (ML)	√ (91.5%)	√ (4.2%)
Random Forest (ML)	√ (93.1%)	× (3.6%)
k-Means Clustering (Unsupervised)	× (87.6%)	× (5.1%)
Deep Neural Network (DNN)	√ (95.4%)	√ (2.8%)
Reinforcement Learning	√ (92.8%)	√ (3.2%)

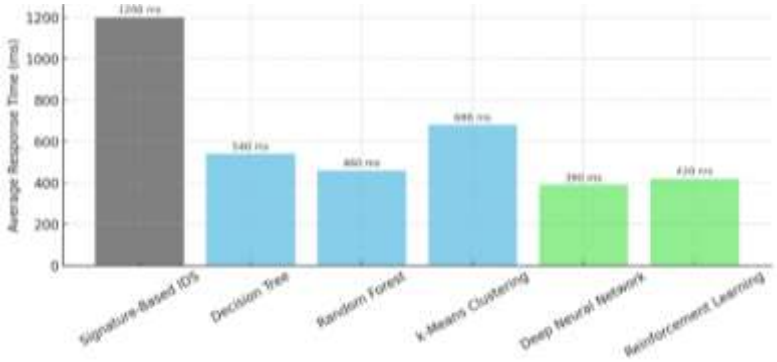

Figure 4: *Real Time Response Capability of cybersecurity Models*

9. Conclusion

The paper examined how the concept of artificial intelligence (AI) is used strategically within the context of contemporary cybersecurity systems and presented how successful it has been in achieving greater threat detection and response potential and how AI has been used to improve a system's overall resilience. The findings support the fact that AI is increasingly playing the role of a powerful tool that revolutionize the processes of cybersecurity and the obstacles that should be overcome to make it widely applicable.

9.1 Key Findings Summary

The study shows that the AI-based models, in particular, deep neural networks and reinforcement learning, are much more effective than traditional signature-based systems with regard to detection accuracy, false positives mitigation, and response time improvement. With the help of a combination of a mixed-method approach (simulations, the use of benchmark datasets (NSL-KDD), and expert interviews. The study will prove the effectiveness of AI in identifying more complex threats and autonomically triggering a relevant response. Such integration with models such as the Cyber Kill Chain and Zero Trust Architecture only increases these advantages.

9.2 Benefits of Artificial Intelligence Vs. a Traditional

The approach of AI has many benefits as compared to the conventional cybersecurity approach. Whereas the traditional systems are built on the use of static signatures and rules, AI models continue to

learn dynamically through the information and eliminate zero-day risks, adapt to change in patterns, and minimize human assistance. AI system reacts in a matter of milliseconds, which clearly cannot be possible with any human or programmed route. AI is used to perform predictive analytics, detect anomalies, and take autonomous decisions, becoming vital in a highly complicated digital environment.

9.3 Deployment and Trust Issues

The adoption of AI in cybersecurity has its drawbacks in spite of the great opportunities it presents. These are the requirements of quality, labeled data, adversarial vulnerability and explainability of complicated models. There is still an issue of trust, so there are numerous professionals who are not sure about using only AI without transparency and human direction. The proper explicability and ethically parsed approach towards models, along with the protection of the AI lifecycle, are the main steps to be undertaken to eliminate these barriers.

9.4 How does hybrid AI-Human

Cyber Defense work in the future? Hybrid defense systems which incorporate the brains of AI with intuition and control on the part of the human being is the future of cybersecurity. AI will continue to absorb routine detection and response activities, and humans will reserve strategic decision making, exceptional handling, and ethical decision making. This partnership spares more efficiency, responsibility, and responsiveness. It is support machine in digital infrastructure protection, AI in the future will become a strategic co-pilot.

10. Future Work

Further studies need to go beyond the existing applications of artificial intelligence and reflect more sophisticated, decentralized, and globally relevant strategies, as AI changes the face of cybersecurity in the future. The steps mentioned below outline possible directions that developed and studied further.

10.1 Decentralized systems with federated learning

The traditional machine learning models depend on centralized data, which remains a threat to privacy and data safety. Federated Learning provides a solution that is decentralized, where AI models trained on numerous edge devices and do not transfer raw data. The applied FL could be studied and implemented in terms of secured distributed systems, which are mobile networks and IoT environments that are equally sensitive in their data applicability and bandwidth limitation.

10.2 Smart Infrastructure and Cities

There is an entreating need to integrate intelligent cybersecurity in the essential civil infrastructure, e.g., in the power grid, traffic systems, and civilian monitoring. The next body of research needs to be on how AI models could be specifically prepared to identify and respond to threats in real-time within highly integrated urban infrastructures where latency, interoperability, and physical security limitations pose unique problems.

10.3 Development of International

Artificial Intelligence Benchmarks Existing standards of AI-based cybersecurity are convenient but not standardized and universal. Further research in the area ought to be aimed at developing standard, current, and internationally approved benchmarks of AI that display contemporary threat patterns. This would allow more uniform evaluations regionally and at institutions to stimulate trust and cooperation in AI development and application.

10.4 Crossover of Blockchain and AI Cybersecurity

Blockchain and AI integration are one of the future vectors of data integrity, model security, and auditability in cyber defense. Blockchain provide tamper-resistant logs, decentralized trust and safe AI model sharing. Further studies that evaluate the potential application of blockchain to supplement AI-based detection systems where transparency, traceability, and resilience are enhanced through blockchain applications in the context of cybersecurity should be undertaken.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.

- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1] Oloyede, J. (2024). Leveraging Artificial Intelligence for Advanced Cybersecurity Threat Detection and Prevention. *Available at SSRN 4976072*.

[2] Fischer, E. A. (2014, December). *Cybersecurity issues and challenges: In brief*.

[3] Khalid, H., Hashim, S. J., Ahmad, S., Hashim, F., & Chaudary, M. A. (2020). Cybersecurity in Industry 4.0 context: Background, issues, and future directions. *The nine pillars of technologies for industry*, *4*, 263-307.

[4] Espinha Gasiba, T., Lechner, U., & Pinto-Albuquerque, M. (2020). Cybersecurity challenges in industry: Measuring the challenge solve time to inform future challenges. *Information*, *11*(11), 533.

[5] Raj, R. K., Anand, V., Gibson, D., Kaza, S., & Phillips, A. (2019, February). Cybersecurity program accreditation: Benefits and challenges. In *Proceedings of the 50th ACM technical symposium on computer science education* (pp. 173-174).

[6] Chingoriwo, T. (2022). Cybersecurity challenges and needs in the context of digital development in Zimbabwe. *British Journal of Multidisciplinary and Advanced Studies*, *3*(2), 77-104.

[7] Liu, L., Sajid, Z., Kravaris, C., & Khan, F. (2024). Detection and analysis of cybersecurity challenges for processing systems. *Process Safety and Environmental Protection*, *185*, 1061-1071.

[8] Bridges, R. A., Huffer, K. M., Jones, C. L., Iannacone, M. D., & Goodall, J. R. (2017, December). Cybersecurity automated information extraction techniques: Drawbacks of current methods, and enhanced extractors. In *2017 16th IEEE international conference on machine learning and applications (ICMLA)* (pp. 437-442). IEEE.

[9] Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., Chen, S., Liu, D., & Li, J. (2020). Performance comparison and current challenges of using machine learning techniques in cybersecurity. *Energies*, *13*(10), 2509.

[10] Fischer, E. A. (2014, December). *Cybersecurity issues and challenges: In brief*.

[11] Khalid, H., Hashim, S. J., Ahmad, S., Hashim, F., & Chaudary, M. A. (2020). Cybersecurity in Industry 4.0 context: Background, issues, and future directions. *The nine pillars of technologies for industry*, *4*, 263-307.

[12] Hasan, M. K., Habib, A. A., Shukur, Z., Ibrahim, F., Islam, S., & Razzaque, M. A. (2023). Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations. *Journal of network and computer applications*, *209*, 103540.

[13] Lezzi, M., Lazoi, M., & Corallo, A. (2018). Cybersecurity for Industry 4.0 in the current literature: A reference framework. *Computers in Industry*, *103*, 97-110.

[14] Camacho, N. G. (2024). The role of AI in cybersecurity: Addressing threats in the digital age. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *3*(1), 143-154.

[15] Abbas, N. N., Ahmed, T., Shah, S. H. U., Omar, M., & Park, H. W. (2019). Investigating the applications of artificial intelligence in cyber security. *Scientometrics*, *121*, 1189-1211.

[16] Aslam, M. (2024). Ai and cybersecurity: an ever-evolving landscape. *International Journal of Advanced Engineering Technologies and Innovations*, *1*.

[17] Wirkuttis, N., & Klein, H. (2017). Artificial intelligence in cybersecurity. *Cyber, Intelligence, and Security*, *1*(1), 103-119.

[18] Carlo, A., Mantı, N. P., WAM, B. A. S., Casamassima, F., Boschetti, N., Breda, P., & Rahloff, T. (2023). The importance of cybersecurity frameworks to regulate emergent AI technologies for space applications. *Journal of Space Safety Engineering*, *10*(4), 474-482.

[19] Zahra, Y., & Sanmorino, A. (2024). Exploring the Evolving Role of AI in Cybersecurity. *European Journal of Privacy Law & Technologies*.

[20] Jun, Y., Craig, A., Shafik, W., & Sharif, L. (2021). Artificial intelligence application in cybersecurity and cyberdefense. *Wireless communications and mobile computing*, *2021*(1), 3329581.

[21] Zhang, Z., Al Hamadi, H., 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.

[22] Patil, P. (2016). Artificial intelligence in cybersecurity. *International journal of research in computer applications and robotics*, *4*(5), 1-5.

[23] Akhtar, M. S., & Feng, T. (2021). An overview of the applications of Artificial Intelligence in Cybersecurity. *EAI endorsed transactions on creative technologies*, *8*(29).

[24] Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, *97*, 101804.

[25] LAZIĆ, L. (2019, January). Benefit from Ai in cybersecurity. In *Proc. 11th Int. Conf. Bus. Inf. Secur.(BISEC)* (pp. 103-119).

[26] Sharifani, K., & Amini, M. (2023). Machine learning and deep learning: A review of methods and applications. *World Information Technology and Engineering Journal*, *10*(07), 3897-3904.

[27] Kumari, J., Kumar, E., & Kumar, D. (2023). A structured analysis to study the role of machine learning and deep learning in the healthcare sector with big data analytics. *Archives of Computational Methods in Engineering*, *30*(6), 3673-3701.

[28] Sharma, N., Sharma, R., & Jindal, N. (2021). Machine learning and deep learning applications-a vision. *Global Transitions Proceedings*, *2*(1), 24-28.

[29] Pramod, A., Naicker, H. S., & Tyagi, A. K. (2021). Machine learning and deep learning: Open issues and future research directions for the next 10 years. *Computational analysis and deep learning for medical care: Principles, methods, and applications*, 463-490.

[30] Geluvaraj, B., Satwik, P. M., & Ashok Kumar, T. A. (2019). The future of cybersecurity: Major role of artificial intelligence, machine learning, and deep learning in cyberspace. In *International Conference on Computer Networks and Communication Technologies: ICCNCT 2018* (pp. 739-747). Springer Singapore.

[31] Taye, M. M. (2023). Understanding of machine learning with deep learning: architectures, workflow, applications and future directions. *Computers*, *12*(5), 91.

[32] Mijwil, M. M., Salem, I. E., & Ismaeel, M. M. (2023). The significance of machine learning and deep learning techniques in cybersecurity: A comprehensive review. *Iraqi Journal For Computer Science and Mathematics*, *4*(1), 10.

[33] Salih, A., Zeebaree, S. T., Ameen, S., Alkhyyat, A., & Shukur, H. M. (2021, February). A survey on the role of artificial intelligence, machine learning and deep learning for cybersecurity attack detection. In *2021 7th International Engineering Conference "Research & Innovation amid Global Pandemic"(IEC)* (pp. 61-66). IEEE.

[34] Gupta, R., Srivastava, D., Sahu, M., Tiwari, S., Ambasta, R. K., & Kumar, P. (2021). Artificial intelligence to deep learning: machine intelligence approach for drug discovery. *Molecular diversity*, *25*, 1315-1360.

[35] Goodfellow, I., Bengio, Y., Courville, A., & Bengio, Y. (2016). *Deep learning* (Vol. 1, No. 2). Cambridge: MIT press.

[36] Abisoye, A., Akerele, J. I., Odio, P. E., Collins, A., Babatunde, G. O., & Mustapha, S. D. (2020). A data-driven approach to strengthening cybersecurity policies in government agencies: Best practices and case studies. *International Journal of Cybersecurity and Policy Studies.(pending publication)*.

[37] Abisoye, A., Akerele, J. I., Odio, P. E., Collins, A., Babatunde, G. O., & Mustapha, S. D. (2025). Using AI and machine learning to predict and mitigate cybersecurity risks in critical infrastructure. *International Journal of Engineering Research and Development*, *21*(2), 205-224.

[38] Gilbert, C., Gilbert, M. A., Dorgbefu, M., Leakpor, D. J., Gaylah, K. D., & Adetunde, I. A. (2025). Enhancing detection and response using artificial intelligence in cybersecurity. *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, *7*(10), 87-104.

[39] Danish, M., & Siraj, M. M. (2025). AI and Cybersecurity: Defending Data and Privacy in the Digital Age. *Journal of Engineering and Computational Intelligence Review*, *3*(1), 25-35.

[40] Radanliev, P. (2025). Cyber diplomacy: defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing. *Journal of Cyber Security Technology*, *9*(1), 28-78.

[41] Elkhodr, M., & Gide, E. (2025). Integrating Generative AI in Cybersecurity Education: Case Study Insights on Pedagogical Strategies, Critical Thinking, and Responsible AI Use. *arXiv preprint arXiv:2502.15357*.

[42] Graham, C. M. (2025). AI skills in cybersecurity: global job trends analysis. *Information & Computer Security*.

[43] Bran, E., Rughiniș, R., Țurcanu, D., & Radovici, A. (2024). AI Leads, Cybersecurity Follows: Unveiling Research Priorities in Sustainable Development Goal-Relevant Technologies across Nations. *Sustainability*, *16*(20), 8886.

[44] Wada, I. U., Izibili, G. O., Babayemi, T., Abdulkareem, A., Macaulay, O. M., & Emadoye, A. (2025). AI-driven cybersecurity in higher education: A systematic review and model evaluation for enhanced threat detection and incident response. *World Journal of Advanced Research and Reviews*, *25*(3), 89-90.

[45] Denis, A., Thomas, A., Robert, W., Samuel, A., Kabiito, S. P., Morish, Z., ... & Mijwil, M. M. (2025). A Survey on Artificial Intelligence and Blockchain Applications in Cybersecurity for Smart Cities. *SHIFRA*, *2025*, 1-45.

[46] Zangana, H. M., Omar, M., & Mohammed, D. (2025). Introduction to Artificial Intelligence in Cybersecurity and Forensic Science. In *Integrating Artificial Intelligence in Cybersecurity and Forensic Practices* (pp. 1-24). IGI Global Scientific Publishing.

[47] Ajayi, A. J., Joseph, S., Metibemu, O. C., Olutimehin, A. T., Balogun, A. Y., & Olaniyi, O. O. (2025). The impact of artificial intelligence on cyber security in digital currency transactions. *Available at SSRN 5137847*.

[48] Radanliev, P., & De Roure, D. (2022). Advancing the cybersecurity of the healthcare system with self-optimizing and self-adaptative artificial intelligence (part 2). *Health and Technology*, *12*(5), 923-929.

[49] Mohamed, S. (2025). AI and Blockchain in Cybersecurity: A Sustainable Approach to Protecting Digital Assets. *Jurnal Ilmiah Informatika dan Komputer*, *2*(1), 1-8.

[50] Thakur, A. S., Alex, T. L., & Nighojkar, A. (2025). Artificial Intelligence in Maritime Anomaly Detection: A Decadal Bibliometric Analysis (2014–2024). *Journal of The Institution of Engineers (India): Series C*, 1-25.

[51] Neoaz, N., Bacha, A., Khan, M., Sherani, A. M. K., Shah, H. H., Abid, N., & Amin, M. H. (2025). AI in Motion: Securing the Future of Healthcare and Mobility through Cybersecurity. *Asian Journal of Engineering, Social and Health*, *4*(1), 176-192.

[52] Mahmud, F., Barikdar, C. R., Hassan, J., Goffer, M. A., Das, N., Orthi, S. M., ... & Hasan, R. (2025). AI-Driven Cybersecurity in IT Project Management: Enhancing Threat Detection and Risk Mitigation. *Journal of Posthumanism*, *5*(4), 23-44.

[53] Schreiber, A., & Schreiber, I. (2025). AI for cyber-security risk: harnessing AI for automatic generation of company-specific cybersecurity risk profiles. *Information & Computer Security*.