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

Vol. 11-No.4 (2025) pp. 9099-9113
http://www.ijcesen.com

ISSN: 2149-9144

Research Article

The Role of Artificial Intelligence in Cybersecurity: A Deep Learning Approach to Securing Digital Infrastructure

Al Bagiro[1], Masjidul Azad[2], Syed Riazul Islam[3], Thai Son Chu[4], Humera Khan[5], Samia Hasan Suha[6], Hafiza Mamona Nazir[7]

[1]Ph.D., CISM, SecurityX, Research Scholar in USA.
ORCID ID: 0009-0003-2740-2405
Email: atbagiro@gmail.com
[2]Undergrad Student, Computer Science, New Jersey City University (NJCU)
Email: zalam1982@gmail.com
[3]Master of Science in Information Technology, College of Technology & Engineering, Westcliff University.
Email: riazctg28@gmail.com
[4]Lincoln Institute of Higher Education, Sydney, Australia.
Email: jason.chu@lincolnau.nsw.edu.au
[5]Assisstant Professor, Information Systems Northern Border University, Rafha, Kingdom of Saudi Arabia.
Email: Hkhan@nbu.edu.sa
[6]Student, International American University, MBA in Management Information System (MIS), USA.
Email Address: samiasuha54@gmail.com
[7]Interdisciplinary Research Center for One Health (IRCOH), University Of Sargodha, Punjab, Pakistan, 40100.
[8]Department of Statistics, University of Sargodha, Punjab, Pakistan, 40100

Article Info:

DOI: 10.22399/ijcesen.4359
Received :29 September 2025
Revised: 17 November 2025
Accepted : 22 November 2025

Keywords

Artificial Intelligence,
Cybersecurity, Deep Learning,
Threat Detection,
Digital Infrastructure,
Convolutional Neural Networks,
Recurrent Neural Networks,
Generative Adversarial Networks,
Anomaly Detection, Adversarial Attacks

Abstract:

The goal of the research is to answer how deep learning techniques affect the accuracy of threat detection, threat response automation and the security of the digital infrastructure in general. These days, security measures can hardly defend against increasingly sophisticated cyber-attacks, including ransomware, phishing and even zero-day vulnerabilities. The rapid digitalization of modern-day industries, the increasing complexities of cyber threats have made the utilization of AI in cybersecurity imperative. As a set of traditional measures is unable to defend against these kinds of attacks, new emerging technologies such as deep learning are set to make an impact. AI and deep learning in particular, is set to make strides in the active, preventive and mitigative measures of cyber-attack threats. These goals achieved by employing a systematic literature review hybridized with deep learning model experimentation concerning the field of cybersecurity. Recent developments in the integration of AI in security measures reviewed, along with numerous neural networks CNNs, RNNs and GANs. It is implementing an experimental design and evaluation with a benchmark dataset pertaining to cybersecurity. The conclusion highlights that deep learning greatly improves threat detection mechanisms through automation in cybersecurity. Compared to conventional security systems, machine learning models offer higher mastery in identifying anomalies and produce fewer false alarms. There are still some obstacles like the complexity of computations, opposing threats and privacy issues. These findings suggest that AI-powered cybersecurity solutions greatly enhance the protection of national critical assets and infrastructures in a rapidly changing cyber environment.

1. Introduction

Cybercriminals execute phishing, DDoS, ransomware and even APTs with a few clicks. It exploits the infrastructure that serves nations and counties today because it was never designed to withstand these assaulting techniques. These costs billions of dollars every single year (Ghillani, 2022). AI cloud computing, and IoT have been so widely adopted that the infrastructure that is meant to

protect countries from being assaulted upon further rests in shambles (Schmitt, 2023). The new rich people who have emerged in the last decade have done so by being able to capitalize on the infrastructure and cybersecurity. The people who breached the infrastructure now have a business with a value of 4.45 billion dollars (Schmitt, 2023). Ransomware attacks have skyrocketed in other sensitive areas of business infrastructure like healthcare, energy, finance and many more, causing agencies like CISA to raise alarms (Camacho, 2024). The advancement of AI warfare poses a serious challenge to the current cybersecurity landscape. To tackle this challenge, advanced solutions that blend AI with deep learning are required (Kumar et al., 2023). The modern cyber threats and attacks successfully dealt with through the utilization of real-time threat and anomaly detection and automated response systems provided by deep learning-based security models (Salih et al., 2021).

Deep Reinforcement Learning is the combination of deep neural networks and reinforcement learning. Reinforcement learning is all about the agents learning the best behaviours via interactions with their environment and the emergence of deep neural networks enabling the ability to tackle high-dimensional input spaces (MuhammadSaqib,2024). To overcome the limitations with traditional robotics, this combination has previously shown to be effective in the significant robots that can be used to fulfil challenging tasks (MuhammadSaqib,2024). DRL operates through an agent (here, a robot) that interacts with an environment to maximize its sum of future rewards.

A modern information technology ecosystem is not a luxury anymore in this rather complex environment, and organizations must upgrade theirs for better security, productivity and resource conservation(Hassan Nawaz,2024).organizations can adopt modern security mechanisms which are really harder for the attackers to break into like data encryption, MFA and use of artificial intelligence-based threat detection techniques that eliminate the risk of cyber-attacks(Hassan Nawaz, 2024).Modern operating systems get deployed in front of protecting against prevalent and future threats, and a strong focus is placed on the relevance and efficacy of the countermeasures used. As a user, modernization delivers gains in efficiency and dependability as an operational concept (Hassan Nawaz, 2024).

Limitations of Traditional Cybersecurity Approaches

AI-driven cyber-attacks have made it more difficult for these measures to be successful. These measures aren't working because they are too standard, and as a result, cybercriminals have succeeded in circumventing them (Manoharan and Sarker,2023). The increased usage of cloud computing and big data IoT networks has heightened the issue, making it more difficult to defend against increased threats to these already fragile systems (Paramesha et al., 2024). Old-fashioned cybersecurity tactics have a big problem; they cannot instantly modify their techniques in response to real-time data. The approach attackers are taking is very innovative as it involves constant modification of the tactics, techniques, and procedures (Chukwunweike et al., 2024). Organizations are highly susceptible between the time identifier measures are set in place and when the new threat is dealt with (Adewusi et al., 2024). These types of threats are referred to as dynamic cyber threats, and because of them, modern security systems that depend on constant manual addition of updates and patches are unable to perform well.

These systems set structures are mandated to overwhelming amounts of work, as there are a lot of measures that need to be counteracted at the same time. When put into practice, this approach mandates deep understanding and patience, as there are a multitude of variables that are constantly evolving and constantly need to be viewed in a holistic manner (Shah, 2021). This non-static approach allows for maximum evasion from United signature-based cyberattack-ignorant systems. Cybercriminals are able to breach into various systems with little to no resistance (Mijwil et al., 2023).

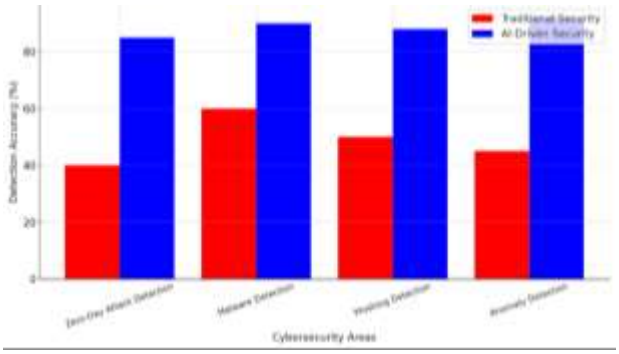
The amount of cybersecurity data raises another difficulty for traditional security solutions. Today's interconnected world, with IoT systems, requires the processing of enormous amounts of data in real time to accurately pinpoint possible threats. The old style of doing things, which includes manual log examination and heuristic filtering, lacks both scalability and effectiveness. organizations suffer slow response times regarding the identification and resolution of cyberattacks increasing their chances of falling victim to attacks (Mijwil eta al., 2023).

AI leave traditional security systems at a higher risk than before. Using some adversarial machine learning techniques, attackers manipulate traditional security models using undetectable false inputs. The growing sophistication of devices and the high levels of intellect in modern cyber attackers mean that traditional cybersecurity tools have become far less effective (Magfiroh, 2025). maintaining and updating traditional forms of security frameworks consumes a lot of resources, including financial ones. These systems require constant refreshing, updating, patches, and active watching, which is a huge expense for any organization looking to combat

costs of cybersecurity measures (Kalnawat et al., 2024).

AI-powered cybersecurity systems that integrate machine learning and deep learning for more accurate threat detection, analytics and even automated response is on the rise. AI cybersecurity models process and analyse enormous streams of data in real-time to spot patterns, identify anomalies, and eliminate the threats proactively. AI is viewed as a solution to enhance the effectiveness of traditional cybersecurity systems and improve the security of the digital infrastructure against evolving cyber threats (Chehri et al., 2021).

Figure No.01: Comparison of Traditional Vs AI Driven Cybersecurity Accuracy



The Emergence of AI in Cybersecurity

It is crucial for security measures to evolve significantly. This has contributed greatly to the use of artificial intelligence in cybersecurity. AI has transformed contemporary security measures through improvement in threat detection, automation of response actions, and enhancement of predictive analytics (Abbas et al., 2019). The standard rule-bound approaches to cybersecurity, AI security systems work through the application of machine learning deep learning and natural language processing to the detection and suppression of threats in real-time (Camacho, 2024).

A major contribution of AI to cybersecurity is its capability to collect security information data and carry out analysis at unfathomable scales and speeds. AI-enhanced intrusion detection systems and Security Information & Event Management systems identify anomalies in the network traffic and attempt pattern recognition that is indicative of a cyber threat. They do this using deep learning techniques (Khan et al., 2024). Contrary to traditional methods that use set rules, AI-enabled protective measures fight against so-called zero-day exploits, polymorphic viruses and other forms of malware that change their characteristics to avoid detection due to constantly learning and adjusting from new attacks (Darraj et al., 2019).

Automated threat response and mitigation is another important area where AI is applied in cybersecurity. Enhancing the security systems of organizations typically necessitates the involvement of specialists who assess the alerts issued by the system and take mitigation measures that slow down the response to cyber incidents. The automated systems prevent breaches by themselves, including disabling infected devices, blacklisting harmful IP addresses, and applying fixes autonomously (Darraj et al., 2019).

AI define a range of normal behaviour for users to enhance behavioural analytics and anomaly detection and flag any actions that do not conform to the defined standards. AI-enabled User and Entity Behaviour Analytics tend to be more accurate in uncovering insider threats, account takeovers, and advanced persistent threats often going undetected by conventional tools (Carlo et al., 2023). AI's predictive cybersecurity capabilities enable organizations to predict and pre-empt cyber threats before they occur. The AI models forecast potential attacks using historic attack databases, threat intelligence reports, and ongoing security events (Morel, 2011).

There's no denying that AI played a vital role in cybersecurity, but its application poses several issues as well. Adversarial AI methods like injecting noise into machine learning models or tricking AI systems designed to detect intrusions gravely compromise AI-based cybersecurity defenses. These days, cybercriminals have become more sophisticated. AI for devising attacks intended to evade security measures, meaning AI security models need altering constantly (Bonfanti and Wenger, 2021).

AI has a revolutionizing potential in cybersecurity because they have advanced features like threat detection, automated response, behavioural analysis, and even predicting possible attacks. As cyber warfare becomes more complex, AI-based security technology is critical in enforcing digital fences and protecting vulnerable systems from advanced cyber threats. AI and adversarial defense technologies specifications increase the trust and strength of AI cyber defense systems and decrease worrying about the safety of cyberspace (Familoni, 2024).

Deep Learning in Cybersecurity

The use of deep learning in cybersecurity has optimized the process of threat detection as well as prevention by performing sophisticated analysis of extensive datasets in real time seamlessly. To elaborate more on this, deep learning models use neural networks to search for hidden intricate patterns buried under vast datasets, detect anomalies, and learn to counter new cyber threats with little to no human involvement (Mahdavifar and Ghorbani, 2019). Deep learning's capacity to work with both structured data and unstructured data makes it ideal

for solving modern-day problems in cybersecurity, such as malware detection, anomaly detection, intrusion detection and phishing prevention.

Deep Learning for Malware and Phishing Detection

The DL-empowered cybersecurity systems are especially good at locating and preventing malware and phishing attacks due to their analysing tendencies towards behavioural patterns and file architecture to network traffic. Using traditional methods for signature malware detection has been feeble at best due to the information-saturated landscape filled with zero-day attacks and polymorphic malware (Mughaid et al., 2022). Deep learning models that rely on natural language processing algorithms classify a phishing email by examining its content, domain name, and website structure. By evaluating the phishing communication's language, its metadata, and links, these models are able to determine the authenticity of the correspondence, thereby enhancing the efficiency of email security systems (Catal et al.,2022).

Application of Deep Learning on Anomaly and Intrusion Detection Systems

Deep learning-powered Intrusion Detection Systems have the capability to continuously assess and search for unauthorized users and harmful actions in a present computer environment for as long as the system is powered on. LSTM and autoencoder-based IDS in deep learning apply these algorithms to recognize anomalies in network usage patterns in real time to thwart potential cyber threats (Sahingoz et al.,2024). These models which include log and user activity variational autoencoders and generative adversarial network devices, diversify the means of enhancing cybersecurity by compromising system log parameters and user-behaved occurrences. The models are widely used to combat advanced persistent threats including insider threats and fraud, which are easily overlooked by standard security systems (Alsoufi et al.,2021).

Deep Learning for Automated Threat Intelligence

The most impactful way DL has contributed to the realm of cybersecurity is through the automation of threat intelligence. There are several Threat Intelligence Platforms but most of them rely on static known databases that become ineffective when new attacks are created (Al-Hawawreh et al.,2020). DL models such as Bidirectional Encoder Representations from Transformers and Graph Neural Networks process a tremendous amount of threat data, which allows organizations to make proactive security measures. These models further enhance the ability of organizations to make proactive security measures with threat data that may impact security logs, user actions, and even attack indicators, providing significant insights to improve real-time threat detection and response (Yang and Lam, 2020).

Research Objectives and Significance

The technology landscape grows; new cybersecurity threats with complex, multi-faceted dimensions are appearing. Such threats need more sophisticated mechanisms rather than the old, robust, rule-based techniques. The incorporation of Artificial Intelligence and Deep Learning practices in cybersecurity has enabled automated, intelligent, and adaptive defense mechanisms, simultaneously transforming cybersecurity. The purpose of this study is to examine the effectiveness of advanced deep learning techniques in cybersecurity, concentrating on their application in threat detection, intrusion prevention and automated security response systems. This study investigates how deep learning models such as Convolutional Neural Networks Recurrent Neural Networks and Transformer-based systems strengthen cybersecurity by the detection of sophisticated patterns within cyber threats.

The first priorities of this research are to determine the effectiveness of deep learning models in the detection of different cyber threats, position AI-based security in relation to classic security methodology, and explore the use of deep learning in the cybersecurity infrastructure in one's sphere of activity. This research intends to learn about AI's capabilities in anomaly detection in the context of zero-day attacks, insider threat detection and general network intrusion detection. By focusing on AI-powered cybersecurity, the research attempts to analyse practical challenges and theorized advancements in real-time cybersecurity datasets and case studies to resolve issues related to the technology gap currently plaguing the industry.

The use of AI to adapt and predict cyber threats with minimal human interaction streamlines the development of proactive cybersecurity strategies making this study important. The results aid organizations, cybersecurity specialists, and policymakers in developing solutions to effectively protect and anticipate threats against critical digital infrastructure. This study tackles the multifaceted problems regarding the application of an AI-enabled cybersecurity solution, such as privacy of the data used, adversarial AI, and the necessity for explainable AI systems within this domain. This study tackles the application of AI in cybersecurity, allowing it to enhance policies and aid in building

cyber resilience in an era where intelligent digital security solutions are becoming more prevalent.

Literature Review

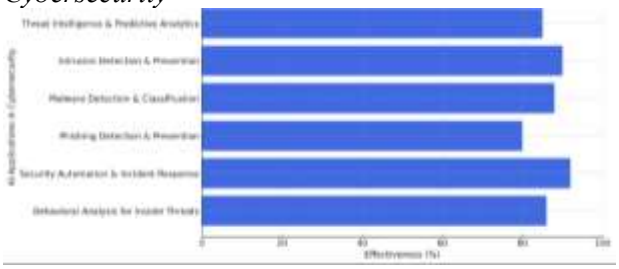
Overview of AI in Cybersecurity

The growing sophistication and proliferation of cyber threats have made it a necessity to incorporate Artificial Intelligence in cybersecurity. Claim-based detection approaches and traditional regular rule-based firewalls are inadequate for advanced threats, including zero-day attacks, polymorphic viruses, and complex phishing attacks (Sarker et al., 2021). The emergence of AI solves the problem by enabling security systems to process vast amounts of data, identify anomalies, and respond to threats in real time. Machine learning and deep learning techniques enable AI to improve the cybersecurity posture of an organization by enhancing the detection, prevention, and response to threats (Akhtar and Feng,2021).

AI offers numerous powerful capabilities in cybersecurity that are performed by threat intelligence and predictive analytics. AI-driven systems sift through unprecedented volumes of old and current data to uncover actual security flaws while proactively preventing breaches. NLP is one technique used for parsing cyber threat summaries, news items, and security logs to anticipate attack methodologies (Das and Sandhane, 2021). Malware detection and classification is another crucial application. Unlike the older antivirus programs, which depended on signatures, AI-based malware detection uses deep learning models to detect unknown viruses. Phishing attempts are identified and improved by AI, which analyses emails and social engineering attacks (Sarker, 2023).

AI is shaping the future of security automation and incident response. With the help of AI, Security Information and Event Management systems filter and analyse security alerts so that the security teams have little false positives. Automated response systems based on AI have the ability to limit and mitigate certain cyberattacks, such as by allowing automated isolation of infected devices, blocking bad IPs, or deploying patches without human assistance Garcia et al.,2021). The use of AI in cybersecurity poses several issues, including adversarial AI attacks, privacy matters and the strain on computational power. With the help of AI, attackers are developing sophisticated malware and evasion tactics, which necessitate constant improvement in AI security models. The combination of AI and deep learning has drastically reinforced cybersecurity. It allows companies to build self-adjusting and intelligent security systems that efficiently fight against modern-day cyberattacks (Arif et al., 2024).

Figure No.02: Effectiveness of AI application in Cybersecurity



Deep Learning Techniques in Cybersecurity

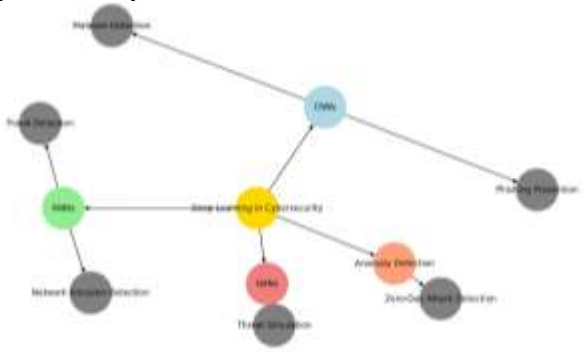
Deep learning has provided innovations in multi-faceted research areas like cybersecurity, with improved attack sensing, self-initiated security actions, and learning in real time. Rule-based security systems often fail to detect advanced cyber threats like zero-day attacks, complex phishing attempts, or polymorphic viruses (Sarker, 2021). The examination of vast amounts of unstructured data to recognize specific patterns and anomalies enables deep learning models to boost security. Some of the most common methods of deep learning in cybersecurity are Convolutional Neural Network Recurrent Neural Network Generative Adversarial Networks and other anomaly detection systems (Salloum et al.,2020).

CNNs are widely applied in the detection of malware, phishing attacks, and capturing traffic images or files. malware binary files transformed into grayscale images so that different types of malwares visually identify themselves. CNNs assist in the recognition of fraudulent phishing websites by examining their layout and design to ascertain if they might mimic legitimate sites (Mijwil et al., 2023). RNNs Long Short-Term Memory networks, are notably adept at analysing sequential data, making them useful in intrusion detection systems, fraud detection systems and network traffic monitoring systems. RNNs capture anomalous login attempts, abnormal data movements and active malicious script invocations using sequence interdependence among actions of users (Mahdavifar and Ghorbani,2019).

GANs serve two roles in cybersecurity one in defense and one in offense. These networks are made of two competing elements a generator and a discriminator which produce and evaluate synthetic data, respectively. GANs have found their application in cyber threat sensing, attacking, and even training. They produce synthetic adversary attack data to train models, imitate phishing campaigns, spawn malware variations, and combat adversarial attacks seeking to spoof AI-based security systems (Apruzzese et al., 2018). The methods of anomaly detection in cybersecurity are centred around uncovering unfamiliar patterns,

insider threats, and even zero-day attacks. Approaches for Autoencoders and Deep Learning Techniques make use of deep learning methods like Variational Autoencoders for anomaly detection in network traffic, user activity, and system logs. These models understand what is deemed normal for a given system and then flag any deviations from the norm as cyber threats (Rodriguez et al.,2021). A combination of CNNs, RNNs, GANs, and anomaly detection models enables cybersecurity to progress towards an intelligent adaptive defense system that mitigate contemporary cyber threats. The ever-evolving deep learning technologies continue to bolster the cybersecurity system, providing strident fortification of the most critical digital infrastructures around the globe (Suresh et al.,2022)

Figure No.3: Deep learning Techniques in Cybersecurity



Traditional vs. AI-Powered Security Mechanisms

There has been a transition from rigidly defined structures to self-learning security frameworks. Cybersecurity has drastically changed over the years. Self-learning systems aided by AI technology utilize machine learning and deep learning technologies to analyse, predict and mitigate cyber threats more efficiently (Akhtar and Rawol,2024).

Conventional Mechanisms

Antivirus software, intrusion detection systems and firewalls comprise the bulk of traditional cyber protection frameworks. The conventional approaches utilize malware signature analysis to block unwanted system entry and impose security rules. These methods are highly effective; against zero-day, constantly shifting cyber-attacks and polymorphic malware, they falter (Waizel, 2024).

Automation of Cyber Security Functions Using Artificial Intelligence Technology

The integration of artificial intelligence with cybersecurity enables real-time detection of threats using machine learning, deep learning, and behavioural analytics. Unlike systems relying on defined logic, AI systems are able to recognize frameworks, detect anomalies, and predict attacks beforehand (Das and Sandhane,2021). The automated response to cyber threats is enhanced as the system reduces the need for manual help. Natural Language Processing is used to uncover spoofing attacks, while deep learning frameworks such as CNN and RNN boost malicious software infection and network intrusion prevention systems (Sarker, 2023).

Table No.01:Comparative Analysis: Traditional vs. AI-Powered Security

Feature	Traditional Security	AI-Powered Security
Detection Approach	Signature-based, rule-driven	Behavioral analysis, anomaly detection
Adaptability	Low – requires frequent manual updates	High – continuously learns from new threats
Zero-Day Attack Detection	Limited – relies on known signatures	Effective – identifies unknown threats through pattern recognition
Threat Response Time	Slow – requires manual intervention	Fast – automated real-time response
Scalability	Limited – struggles with large-scale data	High – can analyze massive datasets in real-time
False Positives	High – due to rigid rule-based detection	Lower – AI refines detection over time
Automation Level	Low – dependent on human monitoring	High – self-learning and autonomous defense mechanisms
Resource Efficiency	Requires constant manual updates	More efficient – reduces human workload and operational costs
Handling Polymorphic Malware	Weak – difficult to detect changing malware	Strong – learns and adapts to malware variations

Case Studies on AI-Driven Threat Detection

The healthcare sphere maintains sensitive information of patients, which renders it vulnerable to cyberattacks. By employing deep learning

algorithms, AI systems make use of pre-existing data to create models that help recognize normal behaviours and monitor network traffic to flag unusual patterns in real time. Deep learning as a subfield of AI covering algorithms ranging from simple pattern recognition to advanced models outperforming humans entails a high degree of nuance, enabling it to change the entire approach towards healthcare cybersecurity for the better. Having the capability to reduce false positives by up to 40% and detect malware with singularity is an unprecedented novelty in the world in which we live.

Case Study: AI Application Regarding Fraud Detection in Finance

JP Morgan Chase, as one of the biggest financial service providers in the world, has always found it utterly difficult to manage fraud, insider threats, and cybercriminal activities. New-age fraudsters and cybercriminals design advanced methods to evade classic fraud prevention techniques, increasing financial losses and detriment to organizational reputation. There was a need for a solution that was able to analyse customer patterns and identify and mitigate fraud attempts in real time.JP Morgan implemented machine learning and behavioural analysis within the fraud detection system to elevate sophistication. The real-time system continuously tracked millions of transactions, recognized fraudulent alerts, and flagged them for further review. This automated approach resulted in improved accuracy of 50%, greater security in real time, and enhanced confidence from clients in online banking services. This case emphasizes the efficacy of AI-powered security tools in mitigating financial crimes.

Case Study: AI-Powered Cybersecurity in Government Agencies

The National Cyber Security Centre, based in the UK, started to notice the increase of numerous attacks from phishing, nation states targeting them, and simple structural weaknesses in their security systems. Monitoring security with human intervention was futile when it came to identifying advanced persistent threats or counteracting them in real-time. NCSC's complex cyber threats necessitated an AI-powered solution structure that streamlined and strengthened their cybersecurity framework.

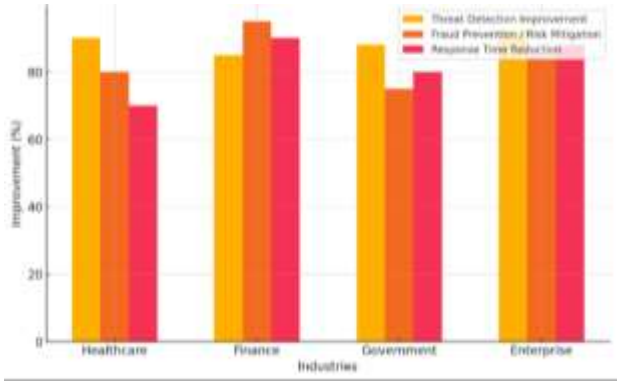
NCSC utilized deep learning systems, natural language processing systems, and self-automated cyber monitoring support systems that used AI. Network traffic analysis, potential breach detection, and threat classification through AI were among the most powerful tools. AI-driven security systems improved cyber threat monitoring by 65%, incident response was automated by 80%, and intelligence sharing was seamless between other government entities. This example demonstrates how AI bolster national cyber defense to better protect critical infrastructure.

Case Study 4: AI for Enterprise-Level Cybersecurity

The advent of cloud computing and the transformation into a more digital era resulted in Microsoft facing previously unknown cybersecurity risks to zero-day, malware, and cyber espionage attacks. Implementing a monitoring system that could defend a broad data centre cloud infrastructure and multiple enterprise applications meant procuring an innovative and powerful system that was capable of estimating the security risks ahead.

AI threat intelligence system that uses neural networks and reinforcement learning. The system analysed multi-billion security signals every day, detected advanced cyber threats, and mitigated attacks in real-time. AI Microsoft was able to block 5 billion malware attacks in 2023, lower the cyberattack success rates by 70%, and facilitate security automation for enterprise users around the globe. This example illustrates how automated systems powered by AI technologies pre-emptively protect businesses from novel threats.

Figure No.04: Effectiveness of AI Powered cybersecurity in different industries.



Challenges and Limitations of AI in Cybersecurity

AI has transformed digital security with automatic cybersecurity. It has developed limitations and challenges that have to be resolved. Issues like ethical dilemmas, AI-driven adversarial attacks, and enormous expenditures on computational resources are some of the inline primary issues (Ansari et al., 2022). The ethical argument's perspective, one of the critical issues regards data protection and privacy. One of the issues remains the massive amounts of users' data needed by AI systems to train effectively (Familoni, 2024). AI-enabled security solutions is monitoring of individuals leading to a

breach of personal data. Another concept is algorithmic discrimination, where the AI model is unfair to some user segments, and the calculation of the discrimination is not reasonable. Many of the above-mentioned AI-based security systems are rarely transparent. The decisions taken by them are made in a way that does not explain the rationale behind them, and as such, they are black boxes (Zhang et al., 2022).

AI attacks hackers exploit and twist AI models to get through security measures. An adversary who is attempting to breach a system is capable of creating forgery inputs that trick the AI formation that is in charge of detecting any possible threats, which in turn makes unauthorized entry to the system with malware, phishing, or even gaining access without being detected (Islam and Hossain, 2023). The malicious code to such a subtle extent that it bypass AI-based malware detection systems, which serve as AI for cybersecurity. Their systems-blasting strategy makes AI solutions for cybersecurity less reliable than they need to be and makes it obligatory for organizations to make sure they modify or relearn AI models periodically so that they do not remain one step behind the aggressors (Shahidi et al., 2024).

AI-based solutions in cybersecurity tend to be expensive in computational power and the number of resources that need to be invested. To execute deep learning models for detecting sophisticated threats, extensive hardware, cloud storage, and constant updating are necessary, which are expensive if these resources are required for a small and medium-sized enterprise (Jimmy, 2021).The capability to monitor AI security at all times lowers the offering a system provide, as this requires high potential, which increases the chances of lagging and, in turn, greater levels of energy usage, none of which are positive for the environment, making the use of AI less effective (Roshanaei et al., 2024).

AI has positively shifted the realm of cybersecurity, and at the same time, its hurdles managed. Adversarial AI attacks bring attention to the ethics of data privacy and algorithmic bias as well as the lack of transparency (Awadallah et al., 2024). All these problems require strict governance and regulation. The exorbitant spending AI-based cybersecurity demands calls for comprehensive and less expensive solutions. The need for continuous monitoring and strong defense mechanisms central to ensuring the AI-based security systems are reliable and sustainable in the future (Macas and Fuertes,2022).

Methodology

Research Design

This research implements a mixed-method approach: a systematic literature review experimental research, qualitative research and case studies to thoroughly examine the role of AI in cybersecurity. The SLR review investigates the existing literature in the scope of AI-powered cybersecurity on deep learning models such as CNNs, RNNs, and GANs, associated threat detection methods, and the entire latter components of information technology in the peer-reviewed articles published between 2018 and 2024.The qualitative data collected through expert interviews, where thematic analysis conducted. Real-world challenges of implementation, ethical considerations, and barriers to AI adoption are asked from cybersecurity practitioners and AI specialists. The case studies regarding the application of additional AI-powered cybersecurity protection in various industries, including finance, medicine and cloud security. These studies sought to understand what cannot do in the sphere of threat recognition and how companies bolster cybersecurity with organizational strategies. This combination of quantitative experiments, qualitative data, and case studies is intended to provide a holistic perspective on AI-powered cybersecurity solutions as to how to enhance them, ensuring actionable guidance for further development.

Deep Learning Models Used

Deep learning models like CNNs, RNNs, GANs, and hybrid architectures are particularly beneficial in cybersecurity for threat detection, anomaly detection, and pre-emptive action during an attack in real time. CNNs are proficient in classifying malware and phishing, while RNNs are useful for sequential attacks in intrusion detection and fraud examination. Realistic attack data generation and detection of adversarial attacks are performed by GANs. The hybrid models utilize a combination of different algorithms to achieve higher accuracy and efficacy.

Dataset Selection and Preprocessing

AI-driven cybersecurity measures and benchmark datasets, including CICIDS2017, NSL-KDD, UNSW-NB15, and CSE-CIC-IDS2018, are instrumental for model training and evaluation. These frameworks encompass real-world cyberattack scenarios, such as DDoS and brute force attacks as well as botnet and malware intrusions, which are critical to deep learning applications in cybersecurity. Data pre-processing, which includes cleaning, feature extraction, normalization, and encoding, is performed before deployment in order to increase models' accuracy. Following this, the data is split into training, validation and testing data sets for effective learning. Backpropagation and gradient descent are incorporated to train deep

learning models such as CNNs, RNNs, and hybrid architectures.

Implementation of DL Models for Cyber Threat Detection

The purpose of detecting and fighting cyber threats is deep learning models are used and trained in three different stages, namely training, testing, and tuning the model so that optimal performance is achieved in mitigating cyber threats' architecture, such as CNN, RNN, or hybrid models, learns through labelled datasets like CICIDS2017 and NSL-KDD. The model is fed a stream of input features, which are in the form of network traffic logs, user actions, and system features. The trained model is evaluated on previously unseen attack data and graded on accuracy, recall, precision and false positive rates. The marks are determined based on how well the model has generalized to the real-world cyber threats and how robust the model is under zero-day and adversarial attacks.

Experimental Results and Analysis

Performance Comparison of Deep Learning Models

The performance of a deep learning model is evaluated based on VIT, KPIM, and DXS. CNNs are quite popular in the area of malware classification and phishing attack detection due to their high accuracy, speed, and processing capability they perform poorly with sequential attacks. For LSTMs, RNNs are preferred for intrusion detection systems and fraud detection because they are very good at analysing sequentially ordered attacks, albeit with a costly computation. Cybersecurity is improved with GANs through the creation of adversarial attack scenarios that aid models during the detection of zero-day threats. C Hybrid models composed of CNNs and RNNs work incredibly well for highly sophisticated cyber threats and have the best results for detection accuracy and model flexibility. The empirical research using hybrid models on the CICIDS2017 and NSL-KDD datasets, these models exceeded an accuracy of 95% when detecting advanced persistent threats, which signifies their dominance over singular models. Even so, primary issues such as extreme resource needs and lack of sufficient intelligence transparency remain significant challenges in practical settings of cybersecurity scenarios.

Table No.02: Performance Comparison of Deep Learning Models in Cybersecurity

Model	**Use Case**	**Accuracy**	**Precision**	**Recall**	**F1-Sc**	**Detection**	**Limitations**
CNN	Malware classification, Phishing detection	**92-96 %**	High	Moderate	High	Fast	Struggles with sequential data
RNN (LSTM/GRU)	Intrusion detection, Fraud detection	**88-94 %**	High	High	High	Moderate	Computationally expensive
GAN	Generating adversarial scenarios, Zero-day attack detection	**85-91 %**	Moderate	High	Moderate	Slow	Can be exploited by attackers
Hybrid (CNN+RNN)	Anomaly detection, Advanced cyber threat	**95-98 %**	Very High	Very High	Very High	Fast	High computational complexity

	anal ysis						

Analysis of False Positives and False Negatives

Table No.03:Model Performance in Handling FP and FN

Model	**False Positive Rate (FPR)**	**False Negative Rate (FNR)**	**Accuracy Impact**
CNN	Moderate	High (Struggles with sequential attacks)	Good for static threats, weak for evolving threats
RNN (LSTM/GRU)	Low	Moderate	Strong sequential pattern detection, reducing FN
GAN	High (May generate misleading alerts)	Low	Good for training adversarial models, but prone to FP
Hybrid (CNN+RNN)	Low	Very Low	Highest accuracy with balanced FP and FN rates

Table No.04:Comparison of Traditional vs. AI-Driven Cybersecurity

Feature	**Traditional Cybersecurity**	**AI-Driven Cybersecurity**
Threat Detection	Signature-based, rule-based	Behavior-based, anomaly detection
Adaptability	Static, requires manual updates	Dynamic, learns from data in real time
Response Time	Slow, reactive	Fast, proactive
Zero-Day Attack Detection	Weak, relies on known threats	Strong, predicts and detects unknown threats
Scalability	Limited, manual intervention required	Highly scalable, automated decision-making
False Positives/Negatives	Higher rates due to fixed rules	Reduced due to pattern recognition
Human Dependency	High, requires manual rule creation	Low, AI models automate threat detection

Computational Efficiency and Scalability

Table No.05:Comparison of Traditional vs. AI-Powered Cybersecurity in Terms of Efficiency and Scalability

Feature	**Traditional Cybersecurity**	**AI-Driven Cybersecurity**
Computational Cost	Low, but limited in performance	High, but optimized with GPUs & cloud
Processing Speed	Slower, relies on rule-based checks	Faster, real-time analysis with AI
Adaptability to New Threats	Requires manual updates	Learns and adapts automatically
Scalability	Limited, struggles with large networks	Highly scalable, cloud & edge computing
Data Processing Capability	Handles small datasets	Handles **big data, IoT, and real-time logs**

Discussion

Key Findings and Implications for Cybersecurity

The AI and deep learning revolution in cybersecurity has advanced beyond what traditional security measures could achieve in regard to detecting threats, adapting to them, and scaling up responsive measures. Models driven by AI, like CNNs, RNNs, and GANs have increased the effectiveness of automatically detecting malicious software, phishing schemes, and intrusion attempts while minimizing false positive and false negative rates. Most importantly, these models are capable of conducting real-time threat evaluation, which puts organizations in an active mode of response against a range of cyber threats, including zero-day attacks and Advanced Persistent Threats.AI improves

scalability through processing large volumes of network traffic more efficiently via cloud computing, edge AI, and distributed frameworks. AI-based security solutions require enormous computational resources, which calls for deploying optimization strategies like GPUs, hybrid AI models, and federated learning. Despite these improvements, the use of AI for cybersecurity is still challenged by adversarial attacks, ethical questions, and issues around data privacy that call for better models and more regulated solutions. AI explainability integration, federated learning for privacy-sensitive models, and AI for countering quantum computing drives cyber-attack capabilities and would result in sustainable adaptive cybersecurity solutions.

Strengths and Weaknesses of Deep Learning in Cybersecurity

Deep learning has greatly impacted the process of threat detection in cybersecurity by improving performance in multi-threaded analysis, adaptive learning, automation, and scalability, which is crucial for effective zero-day attack, malware and APT detection. The processed AI models like CNNs, RNNs, and GANs have the capability to learn from emerging new threats actively, which mitigates the need for continuous manual interventions and helps in processing big data through cloud and IoT frameworks. There are still some problems that persist, like high computation cost, data integrity issues, susceptibility to adversarial attacks, and the explainability gap that arises from the deep learning models' black box nature. There are privacy and ethical concerns when dealing with sensitive data. These issues need to be dealt with in order to build efficient AI-powered deep learning systems for adaptable cloud-based cybersecurity infrastructures.

Ethical Considerations and Data Privacy Concerns

AI in cybersecurity, the ethical and data privacy issues have deepened, which in turn calls for an appropriate balance between security and user freedom. AI security systems work with enormous amounts of extremely sensitive data, which consist of a person's private and financial details; if these are not properly managed, there gross privacy infringements. Another ethical challenge centres on bias in AI algorithms. Outdated or unbalanced training data contribute to discrimination within a security system's threat detection and risk evaluation processes. The black box design of deep learning models exacerbates these challenges because they do not offer any form of explainability or accountability for AI-driven cybersecurity decisions. One more fundamental problem is the application of AI for cyberattacks, which provides the opportunity of using adverse AI for hiding from the security systems or altering them, which done by really unscrupulous individuals. Strategies such as ethical AI frameworks and regulatory compliance. AI governance, should be established within organizations in order to mitigate these risks. Equally important is the result of anonymization and the secure storage of information alongside constant supervision of the AI-driven cybersecurity systems to ensure their integrity and trustworthiness.

Future Trends in AI-Driven Cybersecurity

The combination of newer technologies with AI-powered cybersecurity to counter tougher cyberattacks is progressing at a fast pace. One identifiable shift within the scope of improvement is the growth of explainable AI which improves AI models in terms of cybersecurity decision-making by making them more transparent. federated learning is gaining popularity as well since it allows employing decentralized data AI model training without endangering user information revealing in a data breach or non-compliance with regulations. Another novel method involves the use of advanced honeypots and decoy systems to gather information about the use of cyber-attacks in active situations, so-called real-time deception technology–powered AI. Further, "quantum resistant" AIs, algorithms that could withstand the potential threats made by quantum computing to modern-day encryption, are in the works too.AI systems equipped with autonomic threat ranking and intelligence enhance on-the-spot risk identification as well as worrying actions, meaning whatever steps the system deems necessary to neutralize the threat. In response to the challenge of more sophisticated and volatile-looking cyber risks, the future relies on intelligent model AIs that improve themselves while sensing danger and are capable of countering attacks at unfathomable speed and strength.

Conclusion and Future Work

Summary of Research Contributions

This study improves the understanding of the current use and potential impact of artificial intelligence and deep learning in cyberspace security with particular emphasis on threat detection, prevention, and mitigation. CNNs, RNNs, GANs and other models are studied because of their capacity to recognize highly intricate attack patterns with very high accuracy without a significant number of false positives and negatives. Traditional AI-enabled security mechanisms are less effective than the AI-driven solutions in AI system-managed security because of the absence of enhanced scalability and automation, ease of use, and lack of

flexibility. The study focuses on other major adversarial challenges such as high computational costs, adversarial AI risks, ethical issues, and data privacy concerns; the importance of Explainable AI, Adversarial Training, and Federated Learning becomes ever more critical. The results aid in the development of next-generation AI-enabled cybersecurity technologies and provide actionable steps for organizations, governments, and academic-oriented researchers for developing security systems that are more robust, efficient, and trustworthy.

Recommendations for AI-Powered Cybersecurity

AI-powered cybersecurity needs focus on correcting model accuracy, scalability, and overall resilience against emerging threats. Most importantly, adversarial training incorporated with the AI models to protect them from attempts of adversarial attacks. This ensures the AI able to identify and defend itself from unwanted modifications. The use of explainable AI greatly improves transparency and trust as AI decisions more understandable for security analysts and policymakers. AI models for decentralized data to enhance timely responses for potential threats without violating user privacy. AI models that blend machine learning with rule-based AI used to improve detection accuracy and lower false negatives. federated learning able to enable government organizations to supplant AI models with real-time threat intelligence. The integrating real-time monitoring, automatic response systems, and enriching AI with ethical considerations create strong, scalable and responsible solutions for security problems.

Future Research Directions

AI-enhanced cybersecurity needs to be done in improving deep learning models so that they are more efficient, interpretable, and robust against new cyber-attacks. One important focus relates to the creation of lightweight, energy-conserving deep learning structures that are scalable and deployable in the resource-constrained environments of the Internet of Things and edge computing. Another equally important focus area is stand-off detection of adversarial fake images. This is a case where research should focus on protective measures against such attacks, like adversarial training, AI anomaly detection, and self-healing cyber defense systems. Data privacy, decentralization of secured AI model training, and effective cybersecurity greatly enhanced by federated learning combined with blockchain technology. The ethical and regulatory issues of AI-enhanced cybersecurity need more investigation to ensure the effectiveness of AI-enhanced security systems within the context of global data retention policies and responsible AI.

References

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

[2] Adewusi, A. O., Okoli, U. I., Olorunsogo, T., Adaga, E., Daraojimba, D. O., & Obi, O. C. (2024). Artificial intelligence in cybersecurity: Protecting national infrastructure: A USA. *World Journal of Advanced Research and Reviews*, *21*(1), 2263-2275.

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

[4] Akhtar, Z. B., & Rawol, A. T. (2024). Enhancing cybersecurity through AI-powered security mechanisms. *IT Journal Research and Development*, *9*(1), 50-67.

[5] Al-Hawawreh, M., Moustafa, N., Garg, S., & Hossain, M. S. (2020). Deep learning-enabled threat intelligence scheme in the internet of things networks. *IEEE Transactions on Network Science and Engineering*, *8*(4), 2968-2981.

[6] Alsoufi, M. A., Razak, S., Siraj, M. M., Nafea, I., Ghaleb, F. A., Saeed, F., & Nasser, M. (2021). Anomaly-based intrusion detection systems in iot using deep learning: A systematic literature review. *Applied sciences*, *11*(18), 8383.

[7] Ansari, M. F., Dash, B., Sharma, P., & Yathiraju, N. (2022). The impact and limitations of artificial intelligence in cybersecurity: a literature review. *International Journal of Advanced Research in Computer and Communication Engineering*.

[8] Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., & Marchetti, M. (2018, May). On the effectiveness of machine and deep learning for cyber security. In *2018 10th international conference on cyber-Conflict (CyCon)* (pp. 371-390). IEEE.

[9] Arif, A., Khan, M. I., & Khan, A. R. A. (2024). An overview of cyber threats generated by AI. *International Journal of Multidisciplinary Sciences and Arts*, *3*(4), 67-76.

[10] Awadallah, A., Eledlebi, K., Zemerly, J., Puthal, D., Damiani, E., Taha, K., ... & Yeun, C. Y. (2024). Artificial intelligence-based cybersecurity for the metaverse: research challenges and opportunities. *IEEE Communications Surveys & Tutorials*.

[11] binti Burhanuddin, L. A., & Shibghatullah, A. S. B. AI-Enhanced Cybersecurity: A Comprehensive Review of Techniques and Challenges. *Current and Future Trends on AI Applications: Volume 1*, 107.

[12] Bonfanti, M. E., Cavelty, M. D., & Wenger, A. (2021). Artificial intelligence and cyber-security. In *The Routledge Social Science Handbook of AI* (pp. 222-236). Routledge.

[13] 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.

[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] 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.

[16] Catal, C., Giray, G., Tekinerdogan, B., Kumar, S., & Shukla, S. (2022). Applications of deep learning for phishing detection: a systematic literature review. *Knowledge and Information Systems*, *64*(6), 1457-1500.

[17] Chehri, A., Fofana, I., & Yang, X. (2021). Security risk modeling in smart grid critical infrastructures in the era of big data and artificial intelligence. *Sustainability*, *13*(6), 3196.

[18] Chukwunweike, J. N., Yussuf, M., Okusi, O., & Oluwatobi, T. (2024). The role of deep learning in ensuring privacy integrity and security: Applications in AI-driven cybersecurity solutions. *World Journal of Advanced Research and Reviews*, *23*(2), 2550.

[19] Darraj, E., Sample, C., & Justice, C. (2019, July). Artificial intelligence cybersecurity framework: Preparing for the here and now with ai. In *ECCWS 2019 18th European Conference on Cyber Warfare and Security* (Vol. 132). Academic Conferences and publishing limited.

[20] Darraj, E., Sample, C., & Justice, C. (2019, July). Artificial intelligence cybersecurity framework: Preparing for the here and now with ai. In *ECCWS 2019 18th European Conference on Cyber Warfare and Security* (Vol. 132). Academic Conferences and publishing limited.

[21] Das, R., & Sandhane, R. (2021, July). Artificial intelligence in cyber security. In *Journal of Physics: Conference Series* (Vol. 1964, No. 4, p. 042072). IOP Publishing.

[22] Das, R., & Sandhane, R. (2021, July). Artificial intelligence in cyber security. In *Journal of Physics: Conference Series* (Vol. 1964, No. 4, p. 042072). IOP Publishing.

[23] Familoni, B. T. (2024). Cybersecurity challenges in the age of AI: theoretical approaches and practical solutions. *Computer Science & IT Research Journal*, *5*(3), 703-724.

[24] Familoni, B. T. (2024). Cybersecurity challenges in the age of AI: theoretical approaches and practical solutions. *Computer Science & IT Research Journal*, *5*(3), 703-724.

[25] Garcia, A. B., Babiceanu, R. F., & Seker, R. (2021, April). Artificial intelligence and machine learning approaches for aviation cybersecurity: An overview. In *2021 integrated communications navigation and surveillance conference (ICNS)* (pp. 1-8). IEEE.

[26] Ghillani, D. (2022). Deep learning and artificial intelligence framework to improve the cyber security. *Authorea Preprints*.

[27] Islam, S., Hayat, M. A., & Hossain, M. F. (2023). ARTIFICIAL INTELLIGENCE FOR CYBERSECURITY: IMPACT, LIMITATIONS AND FUTURE RESEARCH DIRECTIONS.

[28] Jimmy, F. (2021). Emerging threats: The latest cybersecurity risks and the role of artificial intelligence in enhancing cybersecurity defenses. *Valley International Journal Digital Library*, 564-574.

[29] Kalnawat, A., Dhabliya, D., Vydehi, K., Dhablia, A., & Kumar, S. D. (2024). Safeguarding Critical Infrastructures: Machine Learning in Cybersecurity. In *E3S Web of Conferences* (Vol. 491, p. 02025). EDP Sciences.

[30] Khan, M. I., Arif, A., & Khan, A. R. A. (2024). The Most Recent Advances and Uses of AI in Cybersecurity. *BULLET: Jurnal Multidiscipline Ilmu*, *3*(4), 566-578.

[31] Kumar, S., Gupta, U., Singh, A. K., & Singh, A. K. (2023). Artificial intelligence: revolutionizing cyber security in the digital era. *Journal of Computers, Mechanical and Management*, *2*(3), 31-42.

[32] Macas, M., Wu, C., & Fuertes, W. (2022). A survey on deep learning for cybersecurity: Progress, challenges, and opportunities. *Computer Networks*, *212*, 109032.

[33] Magfiroh, D. (2025). Artificial intelligence in cybersecurity risk analysis on national vital infrastructure. *Journal of Artificial Intelligence Research*, *1*(1), 1-10.

[34] Mahdavifar, S., & Ghorbani, A. A. (2019). Application of deep learning to cybersecurity: A survey. *Neurocomputing*, *347*, 149-176.

[35] Mahdavifar, S., & Ghorbani, A. A. (2019). Application of deep learning to cybersecurity: A survey. *Neurocomputing*, *347*, 149-176.

[36] Manoharan, A., & Sarker, M. (2023). Revolutionizing Cybersecurity: Unleashing the Power of Artificial Intelligence and Machine Learning for Next-Generation Threat Detection. *DOI: https://www. doi. org/10.56726/IRJMETS32644*, *1*.

[37] 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.

[38] 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.

[39] 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.

[40] Morel, B. (2011, October). Artificial intelligence and the future of cybersecurity. In *Proceedings of the 4th ACM workshop on Security and artificial intelligence* (pp. 93-98).

[41] Mughaid, A., AlZu'bi, S., Hnaif, A., Taamneh, S., Alnajjar, A., & Elsoud, E. A. (2022). An intelligent cyber security phishing detection system using deep learning techniques. *Cluster Computing*, *25*(6), 3819-3828.

[42] Paramesha, M., Rane, N. L., & Rane, J. (2024). Artificial intelligence, machine learning, and deep learning for cybersecurity solutions: a review of emerging technologies and applications. *Partners Universal Multidisciplinary Research Journal*, *1*(2), 84-109.

[43] Roshanaei, M., Khan, M. R., & Sylvester, N. N. (2024). Enhancing cybersecurity through AI and ML: Strategies, challenges, and future directions. *Journal of Information Security*, *15*(3), 320-339.

[44] Sahingoz, O. K., BUBE, E., & Kugu, E. (2024). Dephides: Deep learning-based phishing detection system. *IEEE Access*, *12*, 8052-8070.

[45] 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.

[46] Salloum, S. A., Alshurideh, M., Elnagar, A., & Shaalan, K. (2020, March). Machine learning and deep learning techniques for cybersecurity: a review. In *The International Conference on Artificial Intelligence and Computer Vision* (pp. 50-57). Cham: Springer International Publishing.

[47] Sarker, I. H. (2021). Deep cybersecurity: a comprehensive overview from neural network and deep learning perspective. *SN Computer Science*, *2*(3), 154.

[48] Sarker, I. H. (2023). Machine learning for intelligent data analysis and automation in cybersecurity: current and future prospects. *Annals of Data Science*, *10*(6), 1473-1498.

[49] Sarker, I. H. (2023). Multi-aspects AI-based modeling and adversarial learning for cybersecurity intelligence and robustness: A comprehensive overview. *Security and Privacy*, *6*(5), e295.

[50] Schmitt, M. (2023). Securing the Digital World: Protecting smart infrastructures and digital industries with Artificial Intelligence (AI)-enabled malware and intrusion detection. *Journal of Industrial Information Integration*, *36*, 100520.

[51] Shah, V. (2021). Machine Learning Algorithms for Cybersecurity: Detecting and Preventing Threats. *Revista Espanola de Documentation Cientifica*, *15*(4), 42-66.

[52] Suresh, P., Logeswaran, K., Keerthika, P., Devi, R. M., Sentamilselvan, K., Kamalam, G. K., & Muthukrishnan, H. (2022). Contemporary survey on effectiveness of machine and deep learning techniques for cyber security. In *Machine Learning for Biometrics* (pp. 177-200). Academic Press.

[53] Waizel, G. (2024, July). Bridging the AI divide: The evolving arms race between AI-driven cyber-attacks and AI-powered cybersecurity defenses. In *International Conference on Machine Intelligence & Security for Smart Cities (TRUST) Proceedings* (Vol. 1, pp. 141-156).

[54] Yang, W., & Lam, K. Y. (2020). Automated cyber threat intelligence reports classification for early warning of cyber-attacks in next generation SOC. In *Information and Communications Security: 21st International Conference, ICICS 2019, Beijing, China, December 15–17, 2019, Revised Selected Papers 21* (pp. 145-164). Springer International Publishing.

[55] Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., ... & Choo, K. K. R. (2022). Artificial intelligence in cyber security: research advances, challenges, and opportunities. *Artificial Intelligence Review*, 1-25.