International Journal of Engineering Sciences & Research Technology

(A Peer Reviewed Online Journal)
Impact Factor: 5.164

IJESRT

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

IJESRT
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

ASSESSING THE CHALLENGES OF INTEGRATING ARTIFICIAL INTELLIGENCE IN CYBERSECURITY: LIMITATIONS AND OPPORTUNITIES

Thangaraj Petchiappan
Chief Technology Officer -SIMS iLink Digital
Thangaraj.it@gmail.com
ORCID iD: 0009-0008-2082-3350

DOI: 10.5281/zenodo.14001553

ABSTRACT

Cybersecurity teams may fortify their defences against a wide range of threats and assaults with the use of artificial intelligence (AI), which automates mundane tasks, improves reaction times, and increases accuracy. This article analyses the literature systematically and presents a comprehensive examination of AI use cases for cybersecurity. This paper looks at the opportunities and challenges that AI brings to cybersecurity. The necessity of strengthening cybersecurity measures because of the growth of the complexity of cyber threats has led to the extended application of artificial intelligence in cybersecurity. This research also analyses the factors that hinder the successful deployment of AI in cybersecurity, including data quality, bias in machine learning, interpretability of decisions made by the AI systems and the ability of AI to learn new threats in the future. Furthermore, the study raises the question of what exactly AI adds to cybersecurity: threat detection and analysis, predictive analysis, automation of analysis, and quicker response to threats. This paper's analysis of the benefits and risks of AI for cybersecurity is intended for stakeholders interested in optimising the role of AI while also being mindful of its imperfections. The outcomes indicate the imperative to have effective measures for addressing barriers and more effectively leverage AI for improving frameworks for cybersecurity.

KEYWORDS: Artificial intelligence, Machine learning, Deep learning, Cyber security, Cyber-attacks

1. INTRODUCTION

The goal of cyber security is to prevent unauthorised individuals from gaining access to, altering, or damaging computer systems, networks, applications, and data [1][2]. As an additional component, it incorporates a set of measures used to prevent cyberpunk attacks, illegal access, and damage to system networks, programs, and stored data [3][4]. New dangers are always appearing and evolving as ICT develops. There has been tremendous growth in AI, which is concerned with the science and engineering of making computers intelligent[5][2], and it is impacting every facet of life and business. Numerous fields are benefiting from AI, including gaming, manufacturing, healthcare, education, and NLP. Because AI is used for both offensive and defensive purposes in cyberspace, these advancements are felt in cyber security[6][7]. The once-separate domains of cyber security and AI are beginning to intersect in a variety of ways. One example is the development of programs to address data leakage and strengthen system security in the face of attackers' efforts to imitate legitimate processing at the human client level[8][9]. Cyberattacks are becoming more frequent and sophisticated, but organisations' lack of preparedness is a bigger concern, particularly from a commercial standpoint. Some endpoint solutions, such as those relying on sophisticated heuristics or signatures, have the potential to provide cyber-attack defences of 85–95%[10][11]. Figure 1 shows the cyber security.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

Fig. 1. Cybersecurity

Cybercrime has changed from being primarily seen as digital scrawls intended to create chaos to a multibillion-dollar global business that targets top-tier companies, governments, financial institutions, and people. Malicious software programmers perceive an ROI of around 1,425%, according to recent studies [12][13][14]. The cyber security sector is under constant pressure to develop new methods to detect and prevent new threats because cybercriminals are always looking for new ways to breach systems, given the lucrative nature of their profession. The expansion of the internet has been a major factor in the ever-increasing breadth of cyber security and AI use. The dangerous software that hackers use to attack people, organisations, and governments is always evolving and becoming smarter. When standard security measures fall short, there are other threats to consider, such as phishing, password assaults, virus attacks, etc. Generally speaking, cyber security has improved with the advent of AI [15][16]. In addition to assisting with threat detection, AI systems may aid in the prevention of cyberattacks by doing things like classifying events and threats, which frees up experts from mundane but necessary work[17] [18]. Literature evaluations on the many risks addressed by AI approaches make up this investigation's background on AI in cyber security and its applications in cyber security.

A.Organization of the paper
What follows is an outline of the many parts of this paper: Section II gives an overview of cyber security, Section III explains AI fundamentals, Section IV explains how AI is changing cybersecurity, Section V discusses the integration of AI in cyber security, Section VI explains the limitations and challenges of AI integration in cybersecurity frameworks, Section VII reviews the literature, and Section VIII concludes the paper.

2. OVERVIEW OF CYBER SECURITY

The phrase "cybersecurity" refers to the rules, policies, and technologies put in place to protect information and communication networks from harm, unauthorised access, alteration, or exploitation of stored data. A problem is made more difficult by the quick speed of technical innovation and development as well as the quickly changing nature of cyber threats. Emerging as a reaction to this unprecedented threat, cybersecurity solutions powered by AI are assisting security teams in effectively reducing risks and enhancing security. Because AI and cybersecurity are diverse fields, a uniform taxonomy is necessary for analysing literature on AI in cybersecurity. This standardised taxonomy will help researchers and practitioners reach a consensus on the technology processes and services that need AI enhancement for effective cybersecurity[19].

A.Cyber Security Techniques

There are some techniques for cyber security[20]:

- Access control and password security: An essential method of securing our data is the usage of a username and password. When it comes to cyber protection, this can be a starting step.
- Authentication of data: Precautions that must be taken ensure that the documents received are in good condition and, that the document was obtained from a credible and reputable source it was downloaded from. Usually, the anti-virus software on the devices authenticates these documents. Therefore, a strong anti-virus program is also necessary to safeguard the gadgets from infections.
- Malware scanners: This program detects and eliminates viruses and other forms of unwanted code by scanning all of the system's files and documents. Many forms of harmful software are collectively known as malware, including viruses, worms, and Trojan horses.
- Firewalls: Internet threats, including hackers, viruses, and worms, may be mitigated with the use of a firewall, which can be either software or hardware. The firewall checks all incoming and outgoing

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

communications for certain security requirements and does not allow those that do not. Due to this, firewalls are crucial in identifying malicious software.

- Anti-virus software: The term "antivirus software" refers to a specific kind of computer application that can identify and block harmful software like viruses and worms. The auto-update option is standard in most antivirus products; it lets the software download virus profiles automatically so it can scan for newly detected infections right away.

B. Application area of cyber security

Cybersecurity offers defence, intrusion detection, and encryption technologies to provide confidentiality, integrity, and dependability services for many domains. The following sectors are where cyber security is most relevant since social interaction and industry rely heavily on the internet [21][22].

- Cyber security in smart grid: Renewable energy sources, distributed intelligence, and demand response are all part of the smart grid's plan to make the power grid of the future more efficient and reliable by combining state-of-the-art processing and communication technology. Implementing efficient solutions for the energy problem is made possible by the smart grid's decreased reaction time delay, which allows for faster and better services for customers.
- Cybersecurity in vehicular communication: Cybersecurity is an essential component of vehicle-to-vehicle communication systems and infrastructures, which enhances traffic efficiency, passenger comfort, and road safety. It also secures communication channels among vehicles and infrastructure, like traffic control centres or road units, and protects the software and hardware components of the vehicle, like the electronic control unit.
- Cyber security in smart city: An urban region that employs cutting-edge technology and communication infrastructure to raise the standard of living for its residents is known as a "smart city." To protect public safety and privacy as well as the resilience of vital infrastructure, smart cities' increasing dependence on networked systems and gadgets also poses serious cybersecurity threats that need to be addressed.

3. FUNDAMENTAL OF ARTIFICIAL INTELLIGENCE (AI)

A significant determinant of computer decision-making is artificial intelligence. For example, the computer could see questionable activities on the system and block access until the right person gives their approval. These AI techniques rely on ML, a process whereby computer scientists construct algorithms from historical data. The algorithm's design allows it to detect and differentiate between legitimate and fraudulent access. An organisation's security is enhanced by ML technology since it enhances the predictability of assaults and irregularities. The speed and precision with which dangers are detected are unparalleled by humans. ML and AI can, therefore, protect your business against cyberattacks that might end up costing millions. Regardless, security systems need constant updating by firms since hackers adapt to new technologies [23]. However, AI can still learn by sheer force with the help of enormous data and vast processing, even if algorithms don't become any better. Figure 2 shows the AI techniques in cyber security.

AI works in three ways:

- Assisted intelligence, which enhances existing actions.
- People with enhanced intellect are able to do things that would not be able to accomplish otherwise.
- Autonomous intelligence, a characteristic of self-governing machines.

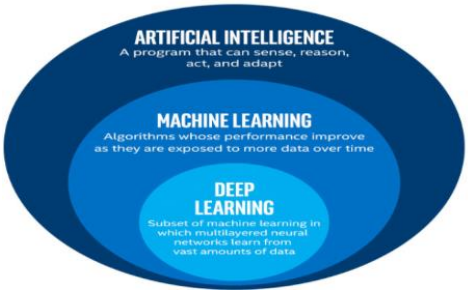

Fig. 2. Overview of Artificial Intelligence

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

Machine Learning: The area of study known as ML allows computers to solve problems and decipher their meaning without the need for a programming language. In other words, it uses past data to make predictions about the future [24][25]. This section's goal is to provide a high-level summary of various ML architectures, classifications, and paradigms. There are different machine learning techniques, as described below and shown in Figure 3:

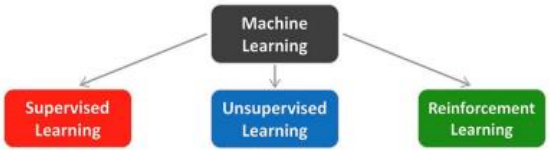

Fig. 3. Machine learning techniques

- Supervised Learning: The training of AI systems in supervised learning takes place on labelled datasets, where each data item is assigned a particular type or category, such as malevolent or benign. Training iteratively teaches the system to correctly associate input data with output labels, which improves its ability to correctly categorise previously unknown data[26][27].
- Unsupervised Learning: In unsupervised learning, AI systems are trained on unlabelled datasets with the goal of finding patterns or structures in the data without direct supervision. Because it may identify departures from typical behaviour without understanding what exactly qualifies as an abnormality, this method is very helpful for anomaly identification[28].
- Reinforcement Learning: AI systems may learn to make judgements by interacting with their surroundings using the trial-and-error learning model known as reinforcement learning[29][30].

Deep Learning: DL is a branch of ML that uses layered artificial neural networks comprised of neurones that communicate with one another. Data that is not yet labelled or classified may be analysed or learnt using Deep Learning's distributed computing capabilities [31][32]. DL models are used by a variety of ML applications to improve data sets, which in turn helps with voice recognition and computer vision. Also, it's employed for tackling complex technological challenges on a big scale[33].

4. THE ROLE OF AI IN TRANSFORMING CYBERSECURITY

To combat the complex cyber threats that contemporary businesses confront, AI is leading the charge in reshaping cybersecurity methods [34]. Security systems are improved in several vital ways when these technologies are integrated into cybersecurity frameworks [32]. AI is mostly excellent at identifying possible security issues early on. Real-time, continuous analysis of massive volumes of network data allows these intelligent systems to spot trends and abnormalities that might point to a security breach[35][36][37]V. The ability of AI to learn to recognise novel and changing dangers makes it a potent weapon against zero-day assaults and sophisticated, persistent threats that usually evade traditional security solutions, which depend on established threat signatures. Figure 4 shows the AI for cyber security.

Fig. 4. AI for cyber security

Beyond detection, AI greatly improves cybersecurity's analysis stage. It may find hidden risks by sorting through and correlating various data points from network traffic to server logs throughout an organisation's digital infrastructure. This data is analysed in a manner and within a time frame that is much faster and more thorough than if the evaluations were left to the analysts [38][39]. Organisations may improve their strategic response by learning about the context and complexity of the attack vectors via this thorough research. Both intelligence and

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

ML are also responsible for making security measures intelligent. Using case studies, it can be noted that the ML models are capable of learning and enhancing their abilities as they work through each attempt at an armed attack. These systems can be able to prevent future attacks by learning the tactics, techniques and processes (TTPs) of the attackers [40]. AI may also be effective in handling security policies in a way that can recommend changes in IDSs, firewalls or other shields in the event of a change of scene in insecurity. A company's digital environment may grow or shrink in size and complexity with the help of AI-powered security solutions [41]. AI and ML systems may boost their monitoring capabilities as data volumes and endpoint counts rise, all without a corresponding rise in human resources or overall expenses. The reason behind this definition is that security must be capable of evolving in tandem with an organisation, as well as the surface area it needs to protect.

The use of AI in cybersecurity strategy allows organisations to enhance their threat detection, analysis, and response capabilities [42]:

- Enhanced Detection Capabilities: AI and ML can process large information and analyse it at a faster rate than human intervention and can identify potential concerns of security at once. This capability makes it possible to identify threats in real time, which is important in preventing the effects of fast-moving threats such as ransomware.
- Predictive Capabilities: AI systems can do more than just detect threats; they can also forecast them by analysing data from a wide variety of sources, such as hacker forums, external threat information, and dark web surveillance. With such prediction capabilities, organisations can work to reinforce their defences and prepare for attacks.
- Automated Response: System reactions to recognised threats may also be automated by AI-driven systems, which can execute specified steps to control and minimise harm. For instance, whenever there is the realisation of a particular network intrusion, then AI systems possess the potential to close off the involved segments in a bid to avoid further transmission of the breach.
- Continuous Learning: These models are operational because they can learn from new data and get better throughout time. The cybersecurity industry depends on this because threat vectors continuously emerge and evolve. By analysing historical data, ML systems may improve their security incident response and attack prediction capabilities.

5. INTEGRATION OF ARTIFICIAL INTELLIGENCE IN CYBER SECURITY

The ability of AI to efficiently analyse large volumes of data, spot trends, and identify possible dangers is making its usage in cybersecurity more and more crucial. The speed and complexity required to tackle current cyberattacks, particularly zero-day threats, are frequently lacking in conventional security measures in this digital age defined by ever-evolving cyber threats[43][44]. The goal of AI is to create intelligent agents by studying human behaviour, knowledge representations, and inference techniques. Agents are able to communicate with one another and share information. The decision-making theory provides the foundation for the knowledge-sharing mechanism that allows agents to solve problems. Each agent is equipped with a decision-making system.

A.Challenges of Artificial Intelligence in Cybersecurity

There are some challenges of AI as below[45]:

- Adapting to evolving threats: Despite advancements in preventive measures, organisations must address the cybersecurity challenges that persist. Cyber threats are always evolving because attackers are constantly developing new methods to circumvent security measures. As technology advances and attackers gain more expertise, organisations must continuously improve their security protocols to manage escalating threats by keeping up-to-date threat information and investing in state-of-the-art security solutions.
- Data Privacy: To find valuable insights and patterns in the data that gadgets give, businesses mostly depend on ML and DL algorithms [46][47]. This procedure necessitates regular training algorithms on enormous data sets collected from many organisations and locations, and one major danger is the transfer of sensitive data to a central training site. The reason for this is the potential for hackers and unauthorised users to access confidential corporate information.
- Scalability: A large amount of data is required for AI systems to learn effectively. Data generated by cybersecurity may be massive and originate from many places, such as recordings of network traffic,

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

system events, and user actions. Processing and analysing the data becomes more complex as its volume increases, which might lead to scalability issues.

- Human-Machine Collaboration: In spite of AI's many positive applications, such as strengthening cybersecurity defences, it brings new and difficult problems, especially when it comes to human-machine interaction [48]. A delicate equilibrium between ML and human supervision is required for AI system integration into cybersecurity operations. Striking this balance is essential for two reasons: first, to fully use AI's promise, and second, to prevent unwanted outcomes caused by automated systems. Cybersecurity experts may rely on AI technologies to supplement their decision-making skills rather than replace them when humans and machines work together effectively [35].

B.Opportunities of Cybersecurity in Artificial Intelligent

The following sections provide a detailed overview of the ways in which different AI approaches have improved cybersecurity measures, outlining their creation and procedures in a categorical manner [49].

- Anomaly Detection: The ability of AI to learn and adapt will contribute to the development of more nuanced anomaly detection systems. Potential threats may be identified by examining user actions and network data for unusual patterns.
- Privacy-Preserving AI: It is critical to find a middle ground between people's right to privacy and the advantages of AI. To help businesses use AI effectively while protecting sensitive information, researchers will focus on creating privacy-preserving AI methods in the future.
- Signature-based Detection: The detection techniques of IDS are built upon a foundation of signature-based detection. It enables intrusion detection systems to swiftly detect malicious activity passing over the network by scouring a database of recognised triggers[50].
- Cloud Security and Encryption: Encryption in the cloud is a data security measure that encrypts plaintext data into an unintelligible ciphertext before storing it in or moving it to another cloud service. One of the best methods to prevent hackers from gaining access to sensitive information while it is on the cloud or while it is in transit is to use this method.
- Threat Intelligence: Effective threat intelligence requires sophisticated methodologies due to the exponential expansion of data supplied by cyber threats. AI has enormous promise for automating the examination of enormous amounts of security data, finding trends, and spotting new dangers[51].
- Explainable AI in Cybersecurity: There are still significant obstacles in the field of cybersecurity related to AI algorithms' transparency and explainability. Improving AI models' explainability is crucial for understanding their decision-making processes and finding their biases and weaknesses.

C.The Benefits of Cyber Security and AI

AI and ML are finding more and more applications in cyber defence. Network traffic vulnerability detection is one area in which AI is finding value. AI systems can detect anomalies in network traffic and notify those responsible for cyber defence of any dangers.

- AI is also capable of analysing vast amounts of data to look for any dangers. In detecting risks that may not be immediately apparent to human analysts, this may be very helpful.
- Automating repetitive processes to save time is another way AI is used for cyber security. AI technologies, for instance, may be used to patch and upgrade systems automatically, freeing up cyber security experts to work on more difficult projects.
- AI is also capable of producing reports and alarms, which provide useful data to support cyber security choices.
- There are a lot of potential advantages for AI in cyber security. The effect of cyberattacks may be lessened by using AI to increase the speed and precision of threat identification and response. The effectiveness of cyber security operations may also be increased by AI, freeing up important time and resources for other purposes.

6. CHALLENGES AND LIMITATIONS OF AI INTEGRATION IN CYBERSECURITY FRAMEWORKS

The study delves into the typical restrictions and difficulties of using AI in cybersecurity. Topics discussed include the ethical implications of automated decision-making, the heavy dependence on data quantity and quality, and the possibility that AI systems may be tricked by complex adversarial assaults. Table I outlines the primary

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

obstacles to deploying AI in cybersecurity, along with descriptions of each obstacle and the effects it has on operations [42].

TABLE I. AI CYBERSECURITY IMPLEMENTATION CHALLENGES

Challenge	Description	Impact Level
Data Quality and Availability	Dependency on high-quality, large datasets	High
Model Bias and Fairness	Risks of biassed AI results because of data that isn't representative	Medium
Adversarial AI Attacks	Dangers of malevolent AI applications versus AI systems	High
Integration and Operational Costs	Expenses related to maintaining and integrating AI/ML	Medium

The integration of AI and ML into cybersecurity frameworks presents both revolutionary advantages and substantial obstacles that must be carefully managed to guarantee efficacy and dependability. A thorough analysis of these difficulties may be found below:

Vulnerability to Sophisticated Adversarial Attacks [52]: Cybersecurity adversarial assaults may disproportionately affect AI and ML models. In order to trick AI models into failing to identify threats, these assaults discreetly alter the data that the models use as input. For example, malevolent parties can write code that is all but invisible but still produces harm by altering just the code identifier. Here, the main issue is the degradation of AI-driven security systems' dependability and credibility. If these systems are readily tricked, they may either fail to recognise real threats, which might result in security breaches, or they would consider normal activities to be threats, which would be inefficient and cause needless inconvenience.

Heavy Reliance on Data Quality and Quantity [53]: The training data further degrades the quality and quantity to determine the efficiency of AI and ML models. Insufficient or prejudiced models may be due to biased or erroneous data. Furthermore, large amounts of data required for training huge models also raise questions about data security and privacy. Algorithms developed by an AI might not detect some types of cyber threats since the AI relies on incomplete or biased data. In addition, accumulating and storing much personally identifiable data could put folks at the mercy of hackers, increasing the risks of cybersecurity.

Ethical Considerations Around Automated Decision-Making [54]: The fear of the unknown poses a problem of ethical issues as more and more systems are powered by artificial intelligence and given the authority to make decisions in cybersecurity. Choices that AI makes concerning which some actions in the network are monitored, or some individuals are denied access affect civil rights and privacy greatly. These questions shake doubts regarding the fairness, accountability or openness of AI operations. Nobody disputes the fact that clear rules for AI decision-making procedures, responsibility for mistakes, or guarantee that these systems do not perpetuate prejudices or violate people’s rights are critically lacking. Overlooking these conditions may expose organisations to legal and image problems besides technical and security problems.

Strategies for Overcoming These Challenges [19]: Several tactics are needed to address these issues:

- Adversarial Training: Avails the problem of adversarial instances to the systems during the training process so that the AI systems can be made more resilient when it comes to such attacks.
- Data Governance: Eliminates prejudicial effects and also safeguards against data loss by ensuring that training data can never be compromised.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

- Ethical AI Frameworks: Helps control the effects of automatic judgement. Maintaining efficacy and fairness requires frequent audits of AI systems, accountability, and the implementation of clear regulations.

7. LITERATURE REVIEW

This section provides a literature review on artificial intelligence in cybersecurity; summary is shown in Table II. Zhang et al. (2022), the four fields of cyber security that this research examined were user access authentication, network situation awareness, harmful behaviour monitoring, and abnormal traffic identification. The studies evaluated herein focused on the use of AI in these contexts. In addition to outlining possibilities and threats to the field, the article argued that human-in-the-loop is crucial, put forward a conceptual model for it, and described its applications. Consequently, a company and I will be working together in the future to put the suggested conceptual model into action and assess its efficacy[55].

Rawat et al. (2022), this research provides a concise overview of AI's uses in many cybersecurity contexts, including the analysis of security using ANNs and the evaluation of the possibility of enhancing defence mechanisms to boost cybersecurity capabilities. A review of the most recent AI software for internet security may reveal the implementation of useful programs. They started by gaining the advantage and many other internet protection areas by using brain organisations. Supplying an AI method that can give security is the major objective of the research. As an added bonus, it zeroes in on the principles, practices, and developments that are changing the face of cyber security[56].

Rehman et al. (2022), The elevated degree of technology in the current world is strongly linked to the rise in cybersecurity risks. It is critical to focus on cybersecurity mat concerns and how to enhance them since modern institutions are undergoing transition. Therefore, the focus of this research study is on AI and how its principles might be used in cybersecurity to enhance data protection. This study draws on descriptive-analytical methods developed for use in earlier studies of AI in cybersecurity. Some suggestions for enhancing cybersecurity are still being considered as the investigation progresses[57].

Vegesna et al. (2023), this study investigates privacy-protecting methods in the context of cybersecurity driven by AI in great detail. The computational burden, data utility, and scalability concerns linked with adopting these strategies are evaluated in the research. Additionally, it highlights the possibilities offered by privacy-preserving AI models, including their ability to improve trust, conformity with regulatory frameworks, and cooperation across many groups without giving away sensitive information. The purpose of this study is to clarify the challenges, trade-offs, and new possibilities associated with implementing privacy-preserving strategies in AI-powered cybersecurity frameworks [58].

Grover and Malhotra (2023), gives a succinct summary of the function of AI in cybersecurity, addressing present issues and suggesting future paths to improve AI's efficacy in safeguarding digital assets. The study assesses current issues facing AI-powered cybersecurity systems, explores the use of AI in-depth, talks about its critical role in cybersecurity, and suggests possible future research and development avenues[59].

Lysenko et al. (2024) demonstrate that AI enables the execution of highly effective solutions, the efficient and rapid identification of cyberattacks, the selection of the ideal reaction to security events, the assessment of their repercussions, and the determination of the method to respond in real-time. In terms of danger detection, risk prevention, and protection automation, the study highlights how effective AI systems are at making decisions. The dangers and difficulties of integrating AI into information security systems have been emphasised by the authors. Given the apparent benefits and potential drawbacks of AI technology, the practical relevance of study results resides in their potential use in establishing an effective cybersecurity system[60].

Adewale et al. (2024), manuscript provides a thorough examination of the transformative role of AI in cybersecurity, including foundational principles, advanced methodologies, and ethical considerations. ML, NLP, and other foundational AI methods are covered in this article. In addition, the paper explores how automation powered by AI may strengthen security postures, reduce human error, and speed up incident response. The ethical and privacy issues surrounding the use of AI in cybersecurity are thoroughly investigated, with a focus on the significance of transparent decision-making, privacy protection, and responsible decision-making. Prospective

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

directions for future research include adversarial ML and zero trust security, which provide chances to strengthen digital resilience against changing attacks[54].

TABLE II. SUMMARY OF THE LITERATURE REVIEW OF THIS INTEGRATING ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

Reference	Focus Area	AI Techniques Used	Cybersecurity Domains	Key Findings	Challenges	Opportunities/ Recommendations
Zhang et al. (2022)	AI in Cybersecurity Domains: User Authentication, Network Awareness, Behavior Monitoring	Machine Learning, User Behavior Analysis	User Access Authentication, Network Awareness	AI's potential in four key cybersecurity domains emphasises the importance of human-in-the-loop and proposes a conceptual model for integration.	Need for effective integration of human oversight in AI systems.	Implement and evaluate proposed model in collaboration with organisations.
Rawat et al. (2022)	AI Utilization in Cybersecurity via Artificial Neural Networks	Artificial Neural Networks, Deep Learning	Threat Detection, Defense Mechanisms	Reviews AI applications with a focus on neural networks for enhancing defence mechanisms in cybersecurity.	Challenges in effectively addressing some cybersecurity issues with current AI tools.	AI strategies for comprehensive threat detection and defence mechanism improvements.
Rehman et al. (2022)	AI's Role in Enhancing Data Protection	Supervised Learning, Data Mining	Data Protection, Threat Identification	Traditional algorithms often fail; AI is essential for modern cybersecurity. Uses past research to analyse AI's effectiveness.	Difficulty in handling complex cyber threats with conventional approaches.	AI-driven data protection improvements and better threat identification strategies.
Vegesna et al. (2023)	Privacy-Preserving AI Techniques in Cybersecurity	Federated Learning, Homomorphic Encryption	Privacy Preservation, Threat Detection	Explores homomorphic encryption, federated learning, and secure multiparty computation for privacy-preserving AI applications.	Computational overhead, scalability, data utility trade-offs in privacy-preserving methods.	Enhancing trust, compliance, and secure collaborations with privacy-preserving AI techniques.
Grover and Malhotra (2023)	AI's Evolution in Cybersecurity	Machine Learning, Data Analytics	Threat Detection, Adaptive Defense	AI's ability to handle vast data and adapt to threats examines challenges in AI integration and future	Challenges in AI-powered cybersecurity systems, including adaptability and complexity.	Enhancing AI models' ability to handle evolving threats; future research in adaptive AI systems.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

				research directions.		
Lysenko et al. (2024)	AI Tools in Cybersecurity for Automated Threat Detection	Expert Systems, Machine Learning	Automated Threat Detection, Incident Response	Proves the effectiveness of AI in automating threat detection and optimising real-time response in cybersecurity.	Risks of human factors in traditional methods; limitations in existing AI capabilities.	Using AI to automate responses, eliminate human error, and implement integrated cybersecurity frameworks.
Adewale et al. (2024)	Fusion of AI with Cybersecurity	Machine Learning, NLP, Automated Systems	Threat Detection, Vulnerability Analysis	AI's impact on threat detection, vulnerability analysis, and incident response. Addresses ethical and privacy considerations in AI for cybersecurity.	Ethical concerns, privacy protection, and responsible AI decision-making challenges.	Focus on AI-driven automation, adaptive risk assessment, and explore trends like adversarial ML and zero trust.

8. CONCLUSION

The safety of people and businesses is greatly dependent on digital technology, making cyber security a must. Various roles, solution categories, use cases, and AI techniques were the focus of the studies conducted on AI in cybersecurity. Integration of Artificial Intelligence in Cybersecurity offers a transformative approach to tackling complex and evolving cyber threats. AI's potential in automating threat detection, predicting attacks, and enhancing incident response can significantly improve the effectiveness of cybersecurity measures. However, the research shows that in order for AI to reach its full potential in this field, a number of issues must be resolved. Issues such as data integrity, bias in AI models, explainability, and the adaptive nature of AI remain significant barriers. Overcoming these obstacles requires a collaborative effort involving the development of transparent algorithms, better data management practices, and robust regulatory frameworks. As AI technology continues to evolve, it will be crucial for cybersecurity professionals to stay updated on its advancements, ensuring AI tools are utilised responsibly and effectively. This study concludes that while AI holds great promise for cybersecurity, careful consideration of its limitations is essential to create a balanced and secure cyber environment.

REFERENCES

1. S. G. A., “The Review of Artificial Intelligence in Cyber Security,” Int. J. Res. Appl. Sci. Eng. Technol., 2022, doi: 10.22214/ijraset.2022.40072.
2. S. Bauskar, “Enhancing System Observability with Machine Learning Techniques for Anomaly Detection,” Int. J. Manag. IT Eng., vol. 14, no. 10, pp. 64–70, 2024.
3. Syed Khurram Hassan and Asif Ibrahim, “The role of Artificial Intelligence in Cyber Security and Incident Response,” Int. J. Electron. Crime Investig., 2023, doi: 10.54692/ijeci.2023.0702154.
4. H. S. Chandu, “A Review of IoT-Based Home Security Solutions: Focusing on Arduino Applications,” TIJER – Int. Res. J., vol. 11, no. 10, pp. a391–a396, 2024.
5. D. Nyale and S. M. Angolo, “A Survey of Artificial Intelligence in Cyber Security,” Int. J. Comput. Appl. Technol. Res., 2022, doi: 10.7753/ijcatr1112.1014.
6. A. M. Shamiulla, “Role of artificial intelligence in cyber security,” Int. J. Innov. Technol. Explor. Eng., 2019, doi: 10.35940/ijitee.A6115.119119.
7. H. S. Chandu, “Enhancing Manufacturing Efficiency: Predictive Maintenance Models Utilizing IoT Sensor Data,” IJSART, vol. 10, no. 9, 2024.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

8. N. N. Abbas, T. Ahmed, S. H. U. Shah, M. Omar, and H. W. Park, "Investigating the applications of artificial intelligence in cyber security," Scientometrics, 2019, doi: 10.1007/s11192-019-03222-9.
9. J. Thomas, K. V. Vedi, and S. Gupta, "The Effect and Challenges of the Internet of Things (IoT) on the Management of Supply Chains," Int. J. Res. Anal. Rev., vol. 8, no. 3, pp. 874–879, 2021.
10. M. Hofstetter, R. Riedl, T. Gees, A. Koumpis, and T. Schaberreiter, "Applications of AI in cybersecurity," in 2020 Second International Conference on Transdisciplinary AI (TransAI), 2020, pp. 138–141. doi: 10.1109/TransAI49837.2020.00031.
11. Sahil Arora and Apoorva Tewari, "Fortifying Critical Infrastructures: Secure Data Management with Edge Computing," Int. J. Adv. Res. Sci. Commun. Technol., vol. 3, no. 2, pp. 946–955, Aug. 2023, doi: 10.48175/IJARSCT-12743E.
12. T. Krishnappa, "A REVIEW ON ARTIFICIAL INTELLIGENCE TECHNIQUES IN PREVENTING CYBER THREATS," Int. J. Eng. Appl. Sci. Technol., 2023, doi: 10.33564/ijeast.2023.v08i01.029.
13. K. Patel, "Exploring the Combined Effort Between Software Testing and Quality Assurance: A Review of Current Practices and Future," Int. Res. J. Eng. Technol., vol. 11, no. 09, pp. 522–529, 2024.
14. K. Patel, "A Review on Software Quality Assurance (QA): Emerging Trends and Technologies," Int. J. Tech. Innov. Mod. Eng. Sci., vol. 10, no. 10, pp. 9–14., 2024.
15. N. Capuano, G. Fenza, V. Loia, and C. Stanzione, "Explainable Artificial Intelligence in CyberSecurity: A Survey," IEEE Access, 2022, doi: 10.1109/ACCESS.2022.3204171.
16. S. Bauskar, "AN PREDICTIVE ANALYTICS OR DATA QUALITY ASSESSMENT THROUGH ARTIFICIAL INTELLIGENCE TECHNIQUES," Int. Res. J. Mod. Eng. Technol. Sci., vol. 06, no. 09, pp. 3330–3337, 2024, doi: https://www.doi.org/10.56726/IRJMETS61568.
17. J. Thomas, K. V. Vedi, and S. Gupta, "Artificial Intelligence and Big Data Analytics for Supply Chain Management," Int. Res. J. Mod. Eng. Technol. Sci., vol. 06, no. 09, 2024, doi: DOI : https://www.doi.org/10.56726/IRJMETS61488.
18. A. Shidawa, A. Achi, G. Kuwunidi Job, F. Shittu, and I. Yakubu, "Survey On The Applications Of Artificial Intelligence In Cyber Security," Int. J. Sci. Technol. Res., 2021.
19. R. Kaur, D. Gabrijelčič, and T. Klobučar, "Artificial intelligence for cybersecurity: Literature review and future research directions," Inf. Fusion, 2023, doi: 10.1016/j.inffus.2023.101804.
20. Y. Zheng, Z. Li, X. Xu, and Q. Zhao, "Dynamic defenses in cyber security: Techniques, methods and challenges," Digit. Commun. Networks, 2022, doi: 10.1016/j.dcan.2021.07.006.
21. W. S. Admass, Y. Y. Munaye, and A. A. Diro, "Cyber security: State of the art, challenges and future directions," Cyber Security and Applications. 2024. doi: 10.1016/j.csa.2023.100031.
22. Pranav Khare and Shristi Srivastava, "Data-driven product marketing strategies: An in-depth analysis of machine learning applications," Int. J. Sci. Res. Arch., vol. 10, no. 2, pp. 1185–1197, Dec. 2023, doi: 10.30574/ijsra.2023.10.2.0933.
23. I. A. Mohammed, "How Artificial Intelligence Is Changing Cyber Security Landscape and Preventing Cyber Attacks: A systematic review," vol. 4, no. 2, p. 659, 2016.
24. H. Sinha, "An examination of machine learning-based credit card fraud detection systems," Int. J. Sci. Res. Arch., vol. 12, no. 01, pp. 2282–2294, 2024, doi: https://doi.org/10.30574/ijsra.2024.12.2.1456.
25. H. Sinha, "Predicting Employee Performance in Business Environments Using Effective Machine Learning Models," Int. J. Nov. Res. Dev., vol. 9, no. 9, pp. 875–881, 2024.
26. H. Sinha, "ANALYZING MOVIE REVIEW SENTIMENTS ADVANCED MACHINE LEARNING AND NATURAL LANGUAGE PROCESSING METHODS," Int. Res. J. Mod. Eng. Technol. Sci. (, vol. 06, no. 08, pp. 1326–1337, 2024.
27. H. Sinha, "The Identification of Network Intrusions with Generative Artificial Intelligence Approach for Cybersecurity," J. Web Appl. Cyber Secur., vol. 2, no. 2, pp. 20–29, Oct. 2024, doi: 10.48001/jowacs.2024.2220-29.
28. H. Sinha, "Benchmarking Predictive Performance Of Machine Learning Approaches For Accurate Prediction Of Boston House Prices : An In-Depth Analysis," ternational J. Res. Anal. Rev., vol. 11, no. 3, 2024.
29. R. Tandon, "The Machine Learning Based Regression Models Analysis For House Price Prediction," Int. J. Res. Anal. Rev., vol. 11, no. 3, pp. 296–305, 2024.
30. K. Ullah et al., "Short-Term Load Forecasting: A Comprehensive Review and Simulation Study with CNN-LSTM Hybrids Approach," IEEE Access, vol. 12, no. July, pp. 111858–111881, 2024, doi: 10.1109/ACCESS.2024.3440631.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

31. H. Sinha, "Advanced Deep Learning Techniques for Image Classification of Plant Leaf Disease," J. Emerg. Technol. Innov. Res. www.jetir.org, vol. 11, no. 9, pp. b107–b113, 2024.
32. S. G. Jubin Thomas, Kirti Vinod Vedi, "Effects of supply chain management strategies on the overall performance of the organisation," Int. J. Sci. Res. Arch., vol. 13, no. 01, pp. 709–719, 2024.
33. R. Tandon, "Face mask detection model based on deep CNN techniques using AWS," Int. J. Eng. Res. Appl., vol. 13, no. 5, pp. 12–19, 2023.
34. S. Thiebes, S. Lins, and A. Sunyaev, "Trustworthy artificial intelligence," Electron. Mark., 2021, doi: 10.1007/s12525-020-00441-4.
35. S. Arora and P. Khare, "THE IMPACT OF MACHINE LEARNING AND AI ON ENHANCING RISK-BASED IDENTITY VERIFICATION PROCESSES," Int. Res. J. Mod. Eng. Technol. Sci., vol. 06, no. 05, pp. 8246–8255, 2024.
36. P. Khare and S. Srivastava, "AI-Powered Fraud Prevention: A Comprehensive Analysis of Machine Learning Applications in Online Transactions," J. Emerg. Technol. Innov. Res., vol. 10, pp. f518–f525, 2023.
37. P. Khare, "Enhancing Security with Voice : A Comprehensive Review of AI-Based Biometric Authentication Systems," vol. 10, no. 2, pp. 398–403, 2023.
38. S. R. Thota and S. Arora, "Neurosymbolic AI for Explainable Recommendations in Frontend UI Design - Bridging the Gap between Data-Driven and Rule-Based Approaches," vol. 11, no. 5, pp. 766–775, 2024.
39. S. R. Thota and S. Arora, "COLLABORATIVE FILTERING AND KNOWLEDGE GRAPHS FOR DATA DISCOVERY," no. 05, pp. 8679–8692, 2024.
40. P. V. Rafel, C. Sanchez-Rivero, and A. Ojeda-Castro, "Navigating the business landscape: challenges and opportunities of implementing artificial intelligence in cybersecurity governance," Issues Inf. Syst., 2023, doi: 10.48009/4_iis_2023_125.
41. M. E. Bonfanti, "Artificial intelligence and the offense-defense balance in cyber security," in Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation, 2022. doi: 10.4324/9781003110224-6.
42. M. Roshanaei, M. R. Khan, and N. N. Sylvester, "Enhancing Cybersecurity through AI and ML: Strategies, Challenges, and Future Directions," J. Inf. Secur., vol. 15, no. 03, pp. 320–339, 2024, doi: 10.4236/jis.2024.153019.
43. J. hua Li, "Cyber security meets artificial intelligence: a survey," Frontiers of Information Technology and Electronic Engineering. 2018. doi: 10.1631/FITEE.1800573.
44. R. Goyal, "EXPLORING THE PERFORMANCE OF MACHINE LEARNING MODELS FOR CLASSIFICATION AND IDENTIFICATION OF FRAUDULENT INSURANCE CLAIMS," Int. J. Core Eng. Manag., vol. 7, no. 10, 2024.
45. K. Meduri, "Enhancing Cybersecurity with Artificial Intelligence: Predictive Techniques and Challenges in the Age of IoT," Int. J. Sci. Eng. Appl., vol. 13, no. 04, pp. 30–33, 2024, doi: 10.7753/ijsea1304.1007.
46. J. Thomas, P. Patidar, K. V. Vedi, and S. Gupta, "Predictive Big Data Analytics For Supply Chain Through Demand Forecasting," Int. J. Creat. Res. Thoughts, vol. 10, no. 06, pp. h868–h873, 2022.
47. K. Patel, "Quality Assurance In The Age Of Data Analytics: Innovations And Challenges," Int. J. Creat. Res. Thoughts, vol. 9, no. 12, pp. f573–f578, 2021.
48. R. Goyal, "An Effective Machine Learning Based Regression Techniques For Prediction Of Health Insurance Cost," Int. J. Core Eng. Manag., vol. 7, no. 11, pp. 49–60, 2024.
49. K. Jabbarova, "Ai and Cybersecurity-New Threats and Opportunities," vol. 5, no. 2, 2023.
50. J. Li, Q. Li, S. Zhou, Y. Yao, and J. Ou, "A review on signature-based detection for network threats," in 2017 9th IEEE International Conference on Communication Software and Networks, ICCSN 2017, 2017. doi: 10.1109/ICCSN.2017.8230284.
51. A. M. Aljuhami and D. M. Bamasoud, "Cyber Threat Intelligence in Risk Management," Int. J. Adv. Comput. Sci. Appl., 2021, doi: 10.14569/ijacsa.2021.0121018.
52. M. Pooyandeh, K. J. Han, and I. Sohn, "Cybersecurity in the AI-Based Metaverse: A Survey," Applied Sciences (Switzerland). 2022. doi: 10.3390/app122412993.
53. S. M. Muneer, M. B. Alvi, and A. Farrakh, "Cyber Security Event Detection Using Machine Learning Technique," Int. J. Comput. Innov. Sci., 2023.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

54. Adewale Daniel Sontan and Segun Victor Samuel, "The intersection of Artificial Intelligence and cybersecurity: Challenges and opportunities," World J. Adv. Res. Rev., 2024, doi: 10.30574/wjarr.2024.21.2.0607.
55. Z. Zhang et al., "Artificial intelligence in cyber security: research advances, challenges, and opportunities," Artif. Intell. Rev., vol. 55, no. 2, pp. 1029–1053, 2022, doi: 10.1007/s10462-021-09976-0.
56. B. S. Rawat, D. Gangodkar, V. Talukdar, K. Saxena, C. Kaur, and S. P. Singh, "The Empirical Analysis of Artificial Intelligence Approaches for Enhancing the Cyber Security for Better Quality," in Proceedings of 5th International Conference on Contemporary Computing and Informatics, IC3I 2022, 2022. doi: 10.1109/IC3I56241.2022.10072877.
57. S. F. U. Rehman, "Practical Implementation of Artificial Intelligence in Cybersecurity – A Study," IJARCCE, vol. 11, no. 11, Oct. 2022, doi: 10.17148/IJARCCE.2022.111103.
58. V. V Vegesna, "Privacy-Preserving Techniques in AI-Powered Cyber Security: Challenges and Opportunities," Int. J. Mach. Learn. …, vol. 5, no. 4, pp. 1–8, 2023.
59. T. Grover and H. Malhotra, "Artificial Intelligence in Cyber Security: Review Paper on Current Challenges Faced by the Industry," Int. J. Sci. Res., vol. 12, no. 12, pp. 741–747, 2023, doi: 10.21275/sr231206140043.
60. Lysenko, Serhii, "The Role of Artificial Intelligence in Cybersecurity: Automation of Protection and Detection of Threats," Econ. Aff., vol. 69, no. 1s, pp. 43–51, Feb. 2024, doi: 10.46852/0424-2513.1.2024.6.