NPRC Journal of Multidisciplinary Research
Vol. 1, No. 4, September 2024. Pages: 121-133
ISSN: 3059-9148 (Online)
DOI: https://doi.org/10.3126/nprcjmr.v1i4.70951

An Overview of AI Applications in Cybersecurity for IT Management

Dipak Adhikari*
PhD Scholar
Lincoln University College, Malaysia
dipsri27@gmail.com

Suman Thapaliya, PhD
IT Department
Lincoln University College, Malaysia
suman@texascollege.edu.np

Corresponding Author*

Received: July 07, 2024; Revised & Accepted: August 29, 2024

Abstract

Background: Cybersecurity serves as a defense mechanism against unauthorized access, theft, information disclosure, and service disruptions for electronic data, networks, and computer systems. Traditional cybersecurity strategies have struggled to counter increasingly sophisticated and automated cyberattacks, necessitating the exploration of advanced solutions such as artificial intelligence (AI).

Aim: This research aims to highlight the role of AI technology and systems in enhancing cybersecurity measures, addressing how AI-based solutions can defend against cyber threats and identifying the associated challenges and future research directions.

Methodology: A systematic literature review was conducted, focusing on recent advancements in AI applications for cybersecurity. Key databases and search engines were utilized to gather relevant articles, which were then filtered based on criteria such as language, publication quality, citation count, and accessibility. The collected literature was analyzed to extract insights on AI methods and their uses in cybersecurity.

Results: The study found that AI offers several benefits in addressing cybersecurity concerns. AI systems can identify novel and complex cyber threats, handle substantial volumes of security data, and establish baselines for normal network behavior to detect deviations. Various

AI techniques, including neural networks, expert systems, intelligent agents, and machine learning, were identified as effective tools in combating cyber threats. AI has demonstrated significant improvements in the detection and prevention of cyberattacks, enhancing overall cybersecurity effectiveness.

Findings: While AI enhances cybersecurity capabilities, it also introduces new challenges such as the need for substantial data and resources, managing false alarms, and vulnerability to adversarial attacks. The study underscores the importance of continuous research to develop robust AI systems that can adapt to evolving cyber threats. Future research should focus on addressing the limitations of AI in cybersecurity, including adversarial threats, data integrity, and human-machine collaboration.

Keywords: Cyber Security, Artificial Intelligence, cyber threat, cyber crime

1. Introduction

Cybersecurity serves as a defence against unauthorized access, theft, information disclosure, and disruption of service for electronic data, networks, and computer systems [1]. Diverse scholars have put forth diverse interpretations of cybersecurity. Sarker and colleagues (2021) provided a comprehensive definition of cybersecurity that takes into account all relevant terminologies. Cybersecurity, as defined by Sarker et al. (2021) [2], is the safety of any that exists in the online realm, including infrastructure, Internet of Things (IOT), applications, networks, databases, and information security. Online safety is defined as an amalgam of techniques covering all aspects of safeguarding private, public, commercial, and government computer data against hackers, attacks, and other adversaries [3]. Over $1 trillion is anticipated to be invested globally in cybersecurity between 2016 and 2021.

For today's generation, using the internet has become a daily necessity. On a daily basis, we shared a tremendous amount of data. Conversely, there is a notable increase in the volume of cyberattacks. Every several months, cybercriminals lower the price of their customised assaults while boosting their potency. Additionally, as automated and sophisticated cyberattacks grow increasingly complex, cybersecurity becomes less effective [4]. Published research indicates that conventional cybersecurity strategies (such as computer security systems and network protection systems) were unable to fend off the ever-evolving, inventive, and transformative cyberattack attempts. As a result, we must figure out how to stop malware and other increasingly emerging cyberthreats. In this case, one cybersecurity strategy that can be effectively applied is artificial intelligence (AI)[5]. Machine learning (ML) and deep learning (DL), two recently developed AI fields, have shown to be extraordinarily successful at thwarting cyberattacks.

Artificial intelligence was initially proposed by John McCarthy in 1956. Intelligent security systems are autonomous thanks to AI. AI's main goal is to teach machines to think, learn, work, perform, and behave like people. Robotics, computer vision, the Internet of Things (IoT), speech recognition, biometric systems, language processing and translation, expert systems, pattern recognition, and other related fields are only a few of the disciplines in which artificial intelligence (AI) provides services[6]. Studying autonomous, intelligent systems, like the human brain, is a major focus of artificial intelligence (AI)[7].

Artificial intelligence is becoming important in cybersecurity in the digital age. Artificial intelligence was initially generally accepted and used in industry, gaming, healthcare, and education. AI can swiftly, correctly, and efficiently analyse massive amounts of electronic data. AI systems, unlike other systems, can predict cyberattacks using previous threats, even if they change. Thus, AI will be utilised to combat security threats. This research aims to highlight AI technology and systems as cybersecurity solutions (Fig. 1). This study addresses the key subject of how AI-based solutions might defend cybersecurity. This study also revealed AI's cybersecurity flaws and urged further investigation. Paper sections are organised as follows: Section 2 presents the literature review and search methodology, Section 3 the overall context of artificial intelligence methods and cybersecurity applications, Section 4 the application of AI to cybersecurity issues, Section 6 the advantages of AI in cybersecurity, Section 8 the challenges, Section 9 the discussion, and Section 10 the study's conclusion and future research.

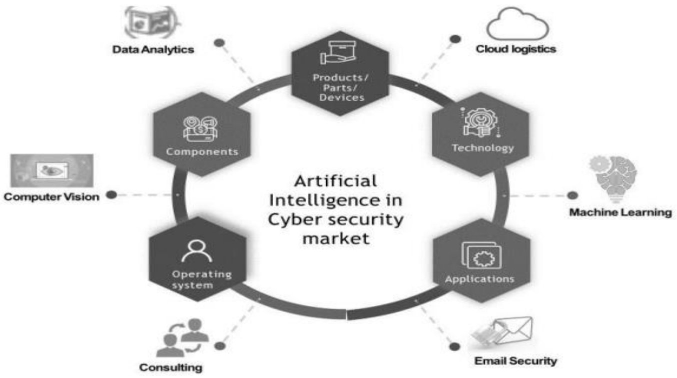

Figure 1: Artificial intelligence applications in the cybersecurity sector

2. Literature Review

Akhtar et al. (2021) highlighted the escalating cyber-attack rates, emphasizing the critical need for cybersecurity in safeguarding electronic data. Through a systematic literature review, they explored AI's potential applications in cybersecurity, citing its superiority in tasks like data analytics. Their findings suggested that AI-based cybersecurity solutions offer significant advantages over traditional methods, showcasing promise in enhancing cyberspace security.

Ansari et al. (2022) examined how artificial intelligence (AI) is changing businesses, industries, and societies. Their research examined AI and cybersecurity, emphasizing the growing importance of cybersecurity as firms adopt information technology. They evaluated AI's diverse effects on cybersecurity and its crucial role in protecting vital data and information through a literature study. The study showed that machine learning technologies improve cybersecurity.

Sarker et al. (2021) provided a comprehensive overview of "AI-driven Cybersecurity," highlighting the importance of AI in defending Internet-connected systems from cyberattacks and unwanted access. The authors proposed employing knowledge representation, natural language processing, deep learning, and machine learning to handle cybersecurity issues intelligently. They advised cybersecurity researchers and industry professionals on intelligent computing and AI-based technical views. AI-based security intelligence modelling automates and improves cybersecurity computing compared to traditional security solutions. In their study, the scientists also suggested various research paths for the topic.

Das et al. (2021) offered a brief summary of AI applications in cybersecurity, emphasizing the importance of automation in managing operations complexity and information size to secure cyberspace. Traditional fixed solutions struggle to protect against security vulnerabilities, hence the article suggested using machine learning in AI. The authors found useful uses for AI in cybersecurity defence, particularly in using neural networks to protect diverse cybersecurity sectors. They stressed the effectiveness of artificial intelligence in cybersecurity, particularly in strategic decision-making where complete information and logical decision help are essential.

Zhang et al. (2022) analyzed XAI cybersecurity, emphasizing the need for ML and DL in AI and Internet-connected device infiltration, malware, and spam filtering. AI surpasses signature and rule-based cybersecurity solutions, but most ML and DL algorithms are opaque, which may undermine security experts' and clients' faith in AI systems. The authors suggested using XAI to improve cybersecurity model openness, reliability, and accuracy. The absence of survey research on XAI in cybersecurity was addressed by providing a complete and updated overview of XAI cybersecurity methodologies to provide significant insights into the sector.

3. Methodology

We gathered the publications for this study using a methodical approach to literature review. A review of the literature was done with an emphasis on the last few years. We choose the current moment for two reasons: **1.** A plethora of published studies about the use of AI in cybersecurity are already accessible online; **2.** Our primary goal is to provide insight into the newest and most cutting-edge applications of AI in cybersecurity. A systematic technique was used to search the literature (Fig. 2). We found the most dependable databases and search engines first. The most targeted and thoroughly investigated keywords with filterable alternatives that were relevant to the paper's content were then developed in the second step. Using these two methods, we were able to compile a library of downloaded literature that included articles regarding the most recent advancements in artificial intelligence applications for cybersecurity. The most recent and closely comparable articles to our subject were found in the library, and we used these to create the current paper. To find the pertinent papers, the following databases and search engines were examined: Microsoft Academic, Web of Science, Research Gate, IEEE Xplore Digital Library, Google, Google Scholar, and Web of Science. All of the articles were chosen based on the following criteria: they had to be written in English, published in esteemed publications, highly cited, and freely accessible (e.g., downloadable in PDF format). All relevant papers' abstracts and conclusions were carefully examined to ensure that they closely matched the subject of our investigation. Lastly, we pinpoint the obstacles and future course of artificial intelligence applications in cybersecurity.

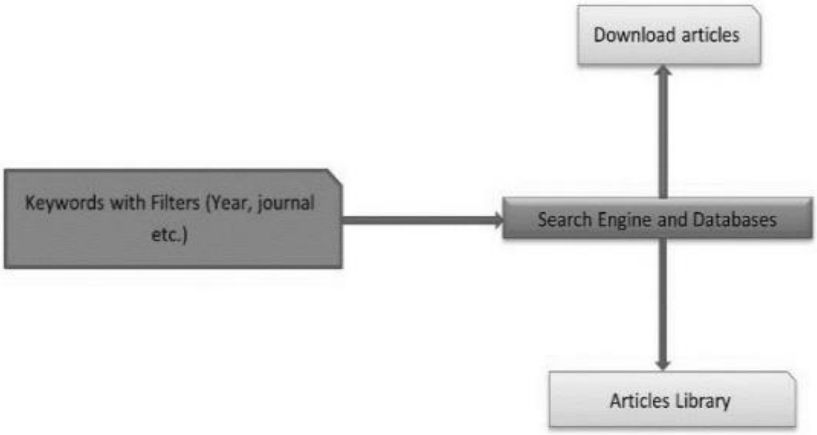
Download articles
Keywords with Filters (Year, journal etc.)
Search Engine and Databases
Articles Library

Figure 2: Methodology of literature collection and search

4. An overview of AI methods and their uses in cybersecurity

However, it is also true that because internet technology and systems are developing so quickly, Attacks and cybercrimes are growing at a startling rate. AI-based cybersecurity solutions are needed to strengthen cyberspace security and combat these hackers' clever techniques. Table 1 provides a quick overview of AI methods and uses.

Technique of AI	**Applications in cybersecurity**
Neural nets	1. For systems that detect and prevent intrusions 2. Extremely fast operation 3. To identify Denial-of-service (DoS) 4. For the purpose of forensic analysis 5. The detection of warmth 6. Ad hoc reasoning
Intelligent t agents	1. Both proactive and reactive 2. Language used by agents to communicate 3. Protection against Distributed Denial-of-Service Attacks (DDoS)
Expert systems	1. To identify network intrusions 2. To assist in making decisions 3. Information repository 4. The engine of inference
Application of Learning	1. Deep learning and machine learning 2. Information extraction 3. Learning both with and without supervision 4. Malware detection and intrusion detection 5. Maps that organize themselves

5. How AI can be used to address cybersecurity concerns

AI offers various benefits to address cybersecurity concerns. A few of these benefits include the following:

(i) As opposed to traditional technology, which was totally dependent on known cyberattacks and mostly focused on the past. Conventional systems have a blind spot during atypical attacks because they are unable to identify changes in the event of a new cyberattack. Attack flexibility variants that are novel and intricate can be identified by AI. AI systems will be able to identify comparable changes more easily in the future. Artificial intelligence (AI) machines have a higher learning and adaption capacity and can identify faster, unusual, and more accurate activities. The increasing sophistication of cyberattacks and the creative and innovative ways employed by cybercriminals make AI systems' capabilities even more crucial.

(ii) AI is capable of handling substantial volumes of security data. Because AI comes with self-contained security mechanisms that are capable of both identifying and thwarting assaults. Unacceptably, security personnel are constantly confronted with data breaches; nonetheless, automated threat detection and response systems have alleviated the burden on professionals. Furthermore, when it comes to handling these hacks, AI is superior to all other approaches. When a lot of security data is generated and transferred across the network, network security analysts will find it harder to identify and monitor attack elements. AI can increase the frequency of problematic behaviour detection and reporting in this case. This can help avoid the need for laborious human analysis by enabling network security officers to respond to scenarios they have never encountered before.

(iii) Over time, AI security systems examine routine network traffic and application behaviour. By identifying potential risks over time, artificial intelligence establishes a baseline of typical patterns. The AI security system will identify any changes or deviations from the typical pattern that indicate an attack.

6. AI techniques used for cybersecurity

To effectively combat threats and cyberattacks, a variety of AI security models can be used, such as deep learning, data mining, expert systems, neural networks, and machine learning. On the internet, intelligent decisions can be made with the help of AI-based techniques. In this paper, each of these AI techniques is listed, and in the following parts, they are all briefly examined.

6.1 Artificial Neural Networks (ANNs)

Artificial Neural Networks (ANNs) learn statistically created in 1957 by Frank Rosenblatt to emulate the activity of neurons in the human brain [13]. ANN approach uses a mathematical equation to simulate neurons, with the model reading large numbers of samples to arrive at a desired value. ANNs have a strong capacity for issue understanding, learning, and solving across a wide range of domains. It can also resolve noisy and incomplete data samples. The early warning, prevention, detection, and response phases of the cyber security system have all made use of ANNs[14]. Intrusion detection systems benefit from ANNs' adaptability. ANNs can assess network traffic flow in cybersecurity, providing breach detection and perimeter protection against cyberattacks [15],[16]. ANNs are able to prevent attacks in the future by using their ability to learn from past network activity. Fig. (3) depicts a typical representation of an ANN.

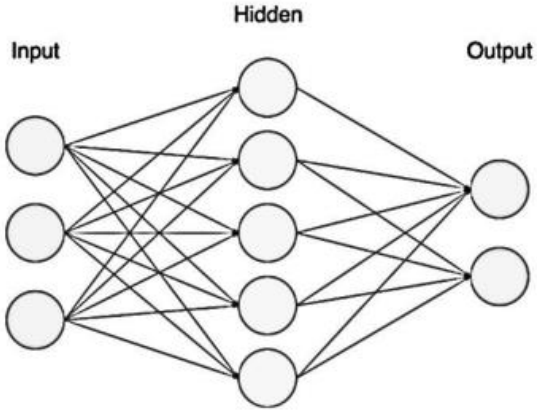

Figure 3: Typical Artificial Neural Network (ANN)

Cybersecurity study [17] used the Cascade Correlation Neural Network (CCNN) to gradually add hidden units to the hidden layer[18]. When new events are found, this approach adds more hidden nodes and trains them with the latest data. In this sense, CCNN provides a flexible and scalable approach. To discover port scanning to mobile networks, the CCNN learns from desktop-platform traffic patterns by only updating the network while disregarding the initial input. This investigation demonstrates how ANN port-scanning identification and evaluation are similar to other methods such as decision trees.

ANNs can identify patterns in extremely nonlinear issues with a high classification rate, which sets them apart from manual methods[19]. ANNs are able to automatically identify normal and problematic network patterns based on previously sent data via the network. Network security equipment like intrusion detection systems, firewalls, and network hubs use ANNS to scan network traffic. The Deep Neural Network (DNN) is an advanced type of artificial neural network (ANN). They have the benefit of protecting the security system from cyberattacks in addition to anticipating their likelihood in the future [20]. An AI-based security program's DNN techniques were used in a study to detect cyberattacks; the findings indicated an 85% success rate [21]. Cyberattack prediction is a new area of cybersecurity that was made possible by DNN's accomplishment.

6.2 Security Expert Systems

Artificial intelligence expert systems assist experts make decisions. Knowledge base and inference engine provide security rules. System chosen by cybersecurity experts follows security rules. Expert systems modelling is used in internet, finance, and medicine. Expert systems range from compact to complex hybrid systems that solve challenging problems. In the cybersecurity expert framework, the inference engine phase extracts new facts and answers from the knowledge base, while the knowledge base phase describes the operational and

domain knowledge of security decision rules. Expert systems may answer many problems relying on logic. One method, "case-based reasoning (CBR) approach," addresses an issue by recalling similar situations. Applying the previous solution to a new problem scenario yields a solution. Thus, new methods are tested to improve the system's precision and learning.
Rule-based systems (RBS) solve expert-set problems. The rule-based system has two subsystems: action and condition. Condition component evaluation determines the best plan of action after analysing the issues. Expert cybersecurity system using rules and recommendations to fight cyberattacks. The security system views a method as safe if it is well-known and effective; if not, it flags it as a threat and terminates it. The inference engine's rules are used by the system to ascertain the machine state if there is no such technique in the knowledge base. The machine has three settings: safe, mild, and hard. A machine's status is reported to management or users based on its current condition and the knowledge base's inference.
In an intelligent cybersecurity framework built to address complex cybersecurity concerns, a rules-based cybersecurity expert system model may be able to make security expert-like choices and use information reasoning. Because of this, cybersecurity expert system modelling can be a useful part of AI-based cybersecurity due to its computational power and capacity for intelligent decision-making.

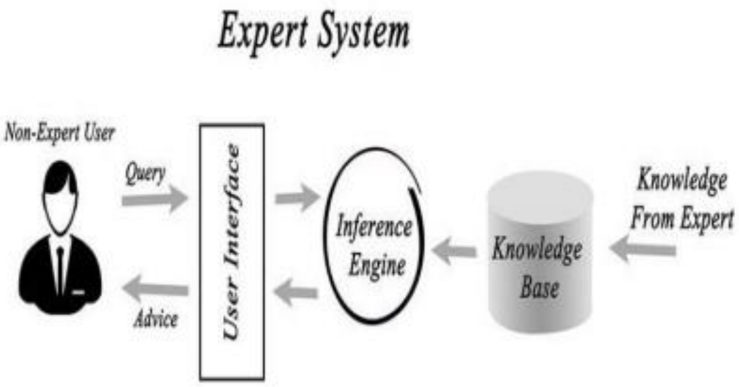

Figure 4: A typical Expert Security System

6.3 Intelligent agents (IAs)

Autonomous intelligent agents, or IAs, make decisions on their own and have a goal. Actuators track the area, while sensors evaluate potential threats. It supervises activities up until the point of completion. These systems can recognise and respond to changes in their domain and are proactive and responsive to other autonomous agents. These adaptable, intelligent agents may interact and learn from their environment. IAs can stop DDoS attacks. How can these agents combat distributed cyberattacks? Artificial "digital police," with mobile intelligent agents, is the solution. To support cyber agent movement and communication, infrastructure must be deployed.

6.4 Search

Search is a critical thinking strategy that can be used in a variety of circumstances, particularly when there isn't another critical thinking strategy available. We also use search strategies on a regular basis as a kind of subliminal problem resolution. Prior to using the search algorithm, one must be familiar with search strategy. These search algorithms are currently present in almost all intelligent programmes, and they have a positive effect on the intelligence system as a whole. AI offers a plethora of search security system approaches, like the widely-used αβ-search estimation. For computer chess, search estimation was created. It uses "isolate and vanquish," a critical thinking strategy used in primitive leadership when two enemies debate the optimal course of action.

6.5 Bio-inspired Computing Method

This innovative field of artificial intelligence uses bioinspired techniques and algorithms to tackle significant environmental and scientific problems. Bio-inspired cyberspace computing approaches include Evolution Strategies, Ant Colony Optimisation, Artificial Immune System, Particle Swamp Optimisation, and Genetic Algorithms. Malware classification employs this strategy. These strategies optimise computer malware classifier parameters and features. For instance, PSO and GA increased malware detection. Another study detected intrusion using fuzzy logic and GA. Glow analysis was used to construct a network segment's digital signature to predict traffic. Network irregularities were identified using fuzzy logic. The university network traffic study showed 96.53 percent accuracy and 0.56 percent false notification.

6.6 Machine learning (ML) and Deep learning (DL) methods

Teaching machines to utilise algorithms to learn and make judgements based on data is known as machine learning. Methods using mathematics to extract data, pattern recognition, and conclusion drawing are closely linked to machine learning. The two primary ML techniques are classification and regression. **1.** Supervised, **2.** Unsupervised, **3.** Semi-supervised, and **4.** Reinforcement Learning are ML technologies.

Another machine learning technique that uses data to teach computers what humans are capable of is called deep learning. Simulations of the brain's data interpretation system achieve this. Deep learning assumes that larger neural networks and more data improve performance.

It has been shown that cybersecurity concerns require the use of ML and DL to be solved. There are many uses for ML techniques in security systems. Examples include botnet tracking, aberrant user behaviour tracking, network anomaly research, and spam filtering. In a similar vein, Deep Learning has demonstrated efficacy in identifying malware and network breaches.

7. Benefits of AI in cybersecurity

Businesses that applied AI to cybersecurity benefited immensely. In cybersecurity, AI has improved ROI for a number of institutions. The AI-powered Siemens Cyber Defence Centre (CDC) from Siemens AG is quick, autonomous, and flexible. He made use of this AWS system. The system's application of AI projected 60,000 attacks every second. The system performance and overall competence were well-managed by less than 12 personnel. Cybersecurity AI can identify emerging dangers by analysing past attacks. This AI method saves time and energy in threat and attack detection. AI reduces threat detection and response costs by 12%. As cybersecurity moves from manual to automated algorithm mitigation, AI can solve huge cybersecurity concerns. AI can detect new, complicated changes in attack extensibility, unlike traditional technology, which focuses largely on already known attackers and incursions, leaving a blind hole during atypical intrusion activities. These limitations of conventional security systems are gone with AI. These days, any changes made to privileged access procedures run the risk of being monitored because privileged internet activity can be observed. AI predictive technologies help security teams stop assaults before they cause damage. A UK startup called Dark Trace used machine learning (ML) to find patterns and threats in the retail, manufacturing, energy, and transportation sectors. AI can enhance network security and handle massive volumes of data. The volume of active security issues overwhelms professionals. Autonomous AI attack detection and response has reduced security group workload. Management of huge amounts of security data collected and sent everyday is difficult for security experts.

Thus, AI can scale up questionable process and activity analysis. Security professionals can profit from substituting manual procedures, which take time to adapt to new events. AI-based systems are more intelligent and capable of defending against threats. AI recognises attacks by looking at the features of the application and the network. With time, AI established a restriction for regular activities after learning the typical traffic conditions. Thus, abnormal deviations indicate attack.

8. Key challenges in AI-driven cybersecurity applications

Data and samples are needed to build AI systems. It is evident that processing this volume of samples requires resources and time. The implementation of AI technology requires sophisticated and expensive resources. Stop clients encountering false alarms. False alarms damage key reactions and disrupt business. A trade-off procedure called fine-tuning reduces false alarms and maintains security.

AI-based systems can be attacked using adversarial inputs, model theft, and data poisoning. Data perception, learning, fine judgements, and final actions are AI model functions. AI systems in complex, interdependent contexts. A false perspective can lead to a bad decision. Each constituent faces different threats and attacks. Classic cyberattacks and training-attacks hit decisions and perception.

Finally, consistency is illogical. Elements should be limited to preserve uncertainty and prevent system misbehaviour. Verifying judgements, logic fixing, and risk analysis for AI and ML components requires an efficient solution. To meet system expectations and respond to various assaults, new approaches must be implemented. AI in cybersecurity may create new dangers, threatening digital security. AI's continuous detection and prevention of cyberattacks has allowed attackers to create increasingly complex threats and attacks. Access to AI approaches lowers technology development costs, which motivates these attackers. Cybercriminals may use the small sum to create more complex programmes. Cybercrime has escalated due to these variables. Human complacency matters. Human complacency is inadequately discussed in AI-based cybersecurity solutions. If cybersecurity uses AI and ML, employees may be less aware of prevention.

AI cybersecurity applications struggle to acquire, manage, and understand unquantified data (structured, semistructured, unstructured, or meta-data), especially for real-world cybersecurity issues.

9. Discussion

In this essay, we discussed AI's cybersecurity applications. AI enables cyberspace investigations. Due to its complexity, number, and flexibility, AI is the best cyberdefense system. According to the literature, AI-based solutions may tackle cybersecurity challenges smartly, unlike traditional security methods that fail in cyberspace. Continuous research on AI applications in cybersecurity suggests that AI papers are growing faster and will attract more attention.

Discussing AI in cybersecurity should include the opposite side. Consider adversarial threats, data poisoning and deception, model theft, and cybercriminals' false positives and negatives when utilising AI in cybersecurity. AI applications expand cybersecurity research despite their limitations.

10.Future research directions

Research has proven that artificial intelligence approaches are subject to adversarial assaults, a major data security risk. AI approaches ignore traditional software analysis and provide new AI attack vectors. Many apps have hidden dependencies, which may be affected. Research is needed to generate new theories, technical concepts, and methods for AI system deployment. Research is needed on environmental vulnerability, tool safety, threat modelling, and human-machine collaboration. AI expertise should guide model and method design. We should abstract and improve cyberattacks using these models. Data availability and integrity, data access control, network privacy, and plastic policy must also be considered.

11.Conclusion

In conclusion, as cyber threats grow more complex and pervasive, traditional cybersecurity methods are increasingly insufficient. Because of this, cybersecurity frameworks must incorporate cutting-edge technology like artificial intelligence (AI). Artificial Intelligence (AI), namely in the forms of Machine Learning (ML) and Deep Learning (DL), greatly improves cybersecurity by offering automatic, intelligent, and adaptive responses to threats.

AI's capabilities in analyzing large volumes of data, recognizing patterns, and adapting to new threats make it a crucial tool in modern cybersecurity. Techniques such as artificial neural networks (ANNs), expert systems, intelligent agents, and bio-inspired computing methods have demonstrated substantial potential in improving cybersecurity measures. These technologies contribute to various applications, including intrusion detection, malware classification, network security management, and proactive defense mechanisms.

Institutions that have integrated AI into their cybersecurity operations report significant benefits, including improved return on investment, enhanced threat detection, and reduced operational costs. For example, Siemens AG's AI-based Cyber Defense Center has shown high efficiency in managing cyber-attacks with minimal human intervention. AI systems can quickly analyze previous threat patterns to identify new threats, saving time and resources that would otherwise be spent on manual investigation.

However, the implementation of AI in cybersecurity is not without challenges. The development and deployment of AI systems require significant data, computational resources, and careful management to avoid issues like false alarms, adversarial inputs, model theft, and data poisoning. The ease of access to AI technologies can also empower cybercriminals, potentially leading to more sophisticated attacks.

Despite these obstacles, AI can improve cybersecurity. Continuous research and development are needed to fix AI-based security weaknesses and strengthen them. To apply AI safely and effectively in cybersecurity, future research should build new theories, technical principles, and human-machine collaboration frameworks. AI technology innovation is needed to secure and resilient digital environments as cyber threats increase. AI can help us create smarter, more resilient cybersecurity systems to protect our digital infrastructure and data.

References

1. Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. *Journal of Digital Forensics, Security and Law*, *12*(2), 8.
2. Sarker, I. H. (2021). Machine learning: Algorithms, real-world applications and research directions. *SN computer science*, *2*(3), 160.
3. Srivastava, S., Benny, B., Ma'am, M. P. G., & Ma'am, N. B. (2021). *Artificial Intelligence (AI) and It's Application in Cyber Security* (No. 5791). EasyChair.
4. Truong, T. C., Diep, Q. B., & Zelinka, I. (2020). Artificial intelligence in the cyber domain: Offense and defense. *Symmetry*, *12*(3), 410.
5. Soni, V. D. (2020). Challenges and Solution for Artificial Intelligence in Cybersecurity of the USA. *Available at SSRN 3624487*.
6. Shamiulla, A. M. (2019). Role of artificial intelligence in cyber security. *International Journal of Innovative Technology and Exploring Engineering*, *9*(1), 4628-4630.
7. Helm, J. M., Swiergosz, A. M., Haeberle, H. S., Karnuta, J. M., Schaffer, J. L., Krebs, V. E., ... & Ramkumar, P. N. (2020). Machine learning and artificial intelligence: definitions, applications, and future directions. *Current reviews in musculoskeletal medicine*, *13*, 69-76.
8. Akhtar, M., & Feng, T. (2021). An overview of the applications of Artificial Intelligence in Cybersecurity. *EAI endorsed transactions on creative technologies*, *8*(29).
9. 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*.
10. Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. *SN Computer Science*, *2*(3), 173.
11. 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.

12. Zhang, Z., Al Hamadi, H., Damiani, E., Yeun, C. Y., & Taher, F. (2022). Explainable artificial intelligence applications in cyber security: State-of-the-art in research. *IEEE Access*, *10*, 93104-93139.
13. McCulloch, W. S., & Pitts, W. (1943). A logical calculus of the ideas immanent in nervous activity. The bulletin of mathematical biophysics, 5(4), 115-133.
14. Kivimaa, J., Ojamaa, A., & Tyugu, E. (2008, October). Graded security expert system. In *International Workshop on Critical Information Infrastructures Security* (pp. 279-286). Berlin, Heidelberg: Springer Berlin Heidelberg.
15. Tyugu, E. (2011, June). Artificial intelligence in cyber defense. In *2011 3rd International conference on cyber conflict* (pp. 1-11). IEEE.
16. Bitter, C., Elizondo, D. A., & Watson, T. (2010, July). Application of artificial neural networks and related techniques to intrusion detection. In *The 2010 International Joint Conference on Neural Networks (IJCNN)* (pp. 1-8). IEEE.
17. Panchev, C., Dobrev, P., & Nicholson, J. (2014). Detecting port scans against mobile devices with neural networks and decision trees. In *Engineering Applications of Neural Networks: 15th International Conference, EANN 2014, Sofia, Bulgaria, September 5-7, 2014. Proceedings 15* (pp. 175-182). Springer International Publishing.
18. Fahlman, S., & Lebiere, C. (1989). The cascade-correlation learning architecture. *Advances in neural information processing systems*, *2*.
19. Stopel, D., Moskovitch, R., Boger, Z., Shahar, Y., & Elovici, Y. (2009). Using artificial neural networks to detect unknown computer worms. *Neural Computing and Applications*, *18*, 663-674.
20. Hinton, G. E., Osindero, S., & Teh, Y. W. (2006). A fast learning algorithm for deep belief nets. *Neural computation*, *18*(7), 1527-1554.
21. Thomson, V. (2016, April 21). Cyber Attacks could be predicted with Artificial Intelligence Help. PatternEX News.
22. Wirkuttis, N., & Klein, H. (2017). Artificial intelligence in cybersecurity. *Cyber, Intelligence, and Security*, *1*(1), 103-119.