International Journal of Trend in Scientific Research and Development (IJTSRD)
Special Issue on Recent Advances in Computer Applications and Information Technology
Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

AI Driven Cyber Security

Chaitanya Bhute, Samiksha Sawarkar

G H Raisoni University, Amravati, Maharashtra, India

Abstract

In the future, intelligent machines will replace or enhance human capabilities in many areas. Artificial intelligence is the intelligence exhibited by machines or software. It is a subfield of computer science. Artificial intelligence is becoming a popular field in computer science as it has enhanced human life in many areas. Artificial intelligence in the last two decades has greatly improved the performance of the manufacturing and service sectors, as well as the field of education. Study in the field of artificial intelligence has given rise to the rapidly growing technology known as expert systems. Application areas of artificial intelligence are having a huge impact on various fields of life, as expert systems are widely used these days to solve complex problems in areas such as education, engineering, business, medicine, weather forecasting, etc. The areas employing artificial intelligence technology have seen an increase in quality and efficiency. This paper gives an overview of this technology and the scope of artificial intelligence in different areas, with special reference to the use of this technology in the field of education, along with its meaning, searching techniques, inventions, and future.

Artificial intelligence (AI) is a powerful technology that helps cybersecurity teams automate repetitive tasks, accelerate threat detection and response, and improve the accuracy of their actions to strengthen the security posture against various security issues and cyberattacks. This article presents a systematic literature review and a detailed analysis of AI use cases for cybersecurity provisioning. The review resulted in 2395 studies, of which 236 were identified as primary. This article classifies the identified AI use cases based on the NIST cybersecurity framework using a thematic analysis approach. This classification framework will provide readers with a comprehensive overview of the potential of AI to improve cybersecurity in different contexts. The review also identifies future research opportunities in emerging cybersecurity application areas, advanced AI methods, data representation, and the development of new infrastructures for the successful adoption of AI-based cybersecurity in today's era of digital transformation and polycrisis.

It is fundamental to comprehend digital protection and expertise to apply it in the cutting edge world, which is fueled by organizations and innovation. Without security, frameworks, essential records, information, and other pivotal virtual articles are powerless. In the same way, attackers do not fall behind as new technologies in cyber security emerge. They are employing more sophisticated hacking methods and focusing on the vulnerabilities of numerous companies. Since military, political, monetary, clinical, and corporate elements accumulate, use, and store immense measures of information on laptops and different gadgets, network safety is urgent. Delicate data, like monetary information, protected innovation, individual data, or different kinds of information for which unapproved access or colleague could raise ominous issues, can make up a sizeable portion of the data. Cybercrime is a type of criminal activity that involves the use of computers or other electronic devices and involves the use of a computer system as a tool, a target, or a place to store evidence of a criminal act. India has strict anti-cybercrime laws in place, but the primary problem facing the nation is low public awareness. In order to prevent giving hackers the upper hand, those combating cybercrime. This research paper provides an overview of Indian cyber regulations, a list of different kinds of cyberattacks and cybersecurity, and an analysis of the state of cyber security in India today.

KEYWORDS: *Detection, Protection, Response, Recovery, Machine Learning, Cyber Attacks, Security Framework, AI in Cyber Securitym Cybersecurity, Artificial Intelligence, Deep Learning, Adversarial Attacks, Meta-Learning, Multi-Agent Systerris, Threat intelligence, Network Security, Cyber Threats.*

1. Introduction

The term cybersecurity refers to a set of technologies, processes and practices to protect and defend networks, devices, software and data from attack, damage or unauthorized access [1]. Cybersecurity is becoming complex because of the exponential growth of interconnected devices, systems and networks. This is exacerbated by advances in the digital economy and infrastructure, leading to a significant growth of cyberattacks with serious consequences. In addition, researchers report the continued evolution of nation-state-affiliated and criminal adversaries, as well as the increasing sophistication of cyberattacks, which are finding new and invasive ways to target even the savviest of targets [2].

This evolution is driving an increase in the number, scale and impact of cyberattacks, and necessitating the implementation of intelligence-driven cybersecurity to provide a dynamic defence against evolving cyberattacks and to manage big data. Advisory organizations, such as the National Institute of Standards and Technologies (NIST), are also encouraging the use of more proactive and adaptive approaches by shifting towards real-time assessments, continuous monitoring and data-driven analysis to identify, protect against, detect, respond to, and catalogue cyberattacks to prevent future security incidents [3].

AI is an intriguing tool that can provide analytics and intelligence to protect against ever-evolving cyberattacks by swiftly analysing millions of events and tracking a wide variety of cyber threats to anticipate and act in advance of the problem. [4] For this reason, AI is increasingly being integrated into the cybersecurity fabric and used in a variety of use cases to automate security tasks or support the work of human security teams. The flourishing field of cybersecurity and the growing enthusiasm of researchers

from both AI and cybersecurity have resulted in numerous studies to solve problems related to the identification, protection, detection, response and recovery from cyberattacks.[5]

Several reviews on cybersecurity and AI applications were published in recent years [9]. However, to the best of our knowledge, there is no comprehensive review that covers state-of-the-art research to explain cybersecurity activities covered by AI techniques and the details of how they are applied. Therefore, our objective was to provide a systematic review, a comprehensive view of AI use cases in cybersecurity, and a discussion of the research challenges related to the adaptation and use of AI for cybersecurity to serve as a reference for future researchers and practitioners.[11] Table 1 shows a comparison of the study with review articles from recent years.

We performed a systematic literature review (SLR) on the use of AI for the provision of cybersecurity, with a particular focus on practical applications within five different cybersecurity functions (Identify, Protect, Detect, Respond and Recover) defined by the NIST cybersecurity framework [10].

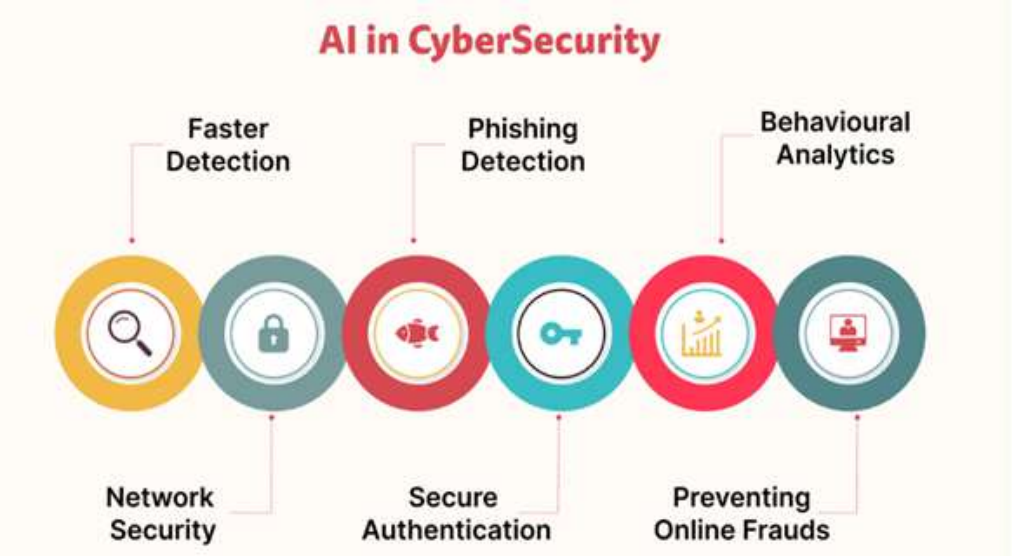


Figure 1: Ai in Cyber Security

2. Literature review

artificial intelligence and cyber security in recent time. Artificial intelligence is very popular in today time because it helps machine to learn and think like human. AI is used in many fields and cyber security is one important field. Researchers said that AI can help to find cyber attacks and protect computer system and data.[6] AI can detect hackers, malware and suspicious activities in network and make system more secure. Some studies show that AI is useful to detect malware, phishing, hacking attempts and other suspicious activities in network. Some authors proposed AI based intrusion detection systems that can monitor network traffic and alert when any abnormal activity is found.[8] Other studies focused on fraud detection and spam detection using AI models.

Many research papers also discussed machine learning and neural networks in cyber security.[4] These techniques help computer to learn from old data and detect new threats automatically. Researchers said that AI can reduce human work in cyber security field.[9] AI systems can do security tasks like monitoring, analyzing logs and responding to threats automatically. This helps security teams to take fast action when any cyber attack happens. Some papers explained that AI can predict cyber attacks before they happen by analyzing patterns and behaviors of attackers.[5]

Organizations like NIST and other cyber security institutes suggested using AI techniques in different security functions such as identify, protect, detect, respond and recover.[7] Some studies compared traditional security methods with AI based methods and found that AI gives better accuracy and faster results.[3] Researchers also discussed challenges like data privacy, false alarms, and need of large data for training AI models.

However, many existing research papers focus only on one part of AI in cyber security and do not give complete overview.[3] Some papers are technical and difficult to understand for beginners. Therefore, there is still need for more research to explain AI driven cyber security in simple way and to study its applications, advantages and future scope.[5]

This research paper studies the role of artificial intelligence in cyber security. It reviews previous research works and explains how AI techniques are used to protect systems, detect attacks and improve security.[3] The paper also discusses future opportunities and challenges of AI driven cyber security. (2023) discuss how adversaries exploit vulnerabilities in generative AI to conduct social engineering attacks, phishing, and automated hacking. The transformative role of generative AI in enhancing threat detection and cyber resilience is further discussed by (Usman et al., 2024), who detail AI's capacity to automate complex cyber-attacks. Despite these risks, generative AI also offers significant defense potential, from threat intelligence automation to secure code generation. Similarly, (Sebastian, 2023) explores how AI-based chatbots, such as ChatGPT, pose potential cyber risks, highlighting examples where malicious actors have exploited vulnerabilities in these systems. Broklyn et al., (2024) argue that while generative AI can be leveraged for defensive measures like automated threat detection, it also introduces new vulnerabilities. Meanwhile, (Ramakrishnan & Chittibala, 2024) examined the convergence of Security Information and Event Management (SIEM), Security Orchestration, Automation, and Response (SOAR), and AI technologies, highlighting their role in proactive cybersecurity framew.

It is fundamental to comprehend digital protection and expertise to apply it in the cutting edge world, which is fueled by organizations and innovation. Without security, frameworks, essential records, information, and other pivotal virtual articles are powerless. In[2] the same way, attackers do not fall behind as new technologies in cyber security emerge. They are employing more sophisticated hacking methods and focusing on the vulnerabilities of numerous companies. Since military, political, monetary, clinical, and corporate elements accumulate, use, and store immense measures of information on laptops and different gadgets, network safety is urgent.[4] Delicate data, like monetary information, protected innovation, individual data, or different kinds of information for which unapproved access or colleague could raise ominous issues, can make up a sizeable portion of the data.[5] Cybercrime is a type of criminal activity that involves the use of computers or other electronic devices and involves the use of a computer system as a tool, a target, or a place to store evidence of a criminal act. India has strict anti-cybercrime laws in place, but the primary problem facing the nation is low public awareness. In order to prevent giving hackers the upper hand, those combating cybercrime.[7] This research paper provides an overview of Indian cyber regulations, a list of different kinds of cyberattacks and cybersecurity, and an analysis of the state of cyber security in India today.[10]

3. Research Methodology

This research uses Systematic Literature Review (SLR) method. SLR is used to find and study all available research papers related to artificial intelligence and cyber security.[1] The main aim of SLR is to understand existing research and find research gaps in this area. It also helps to summarize many research studies in simple way. Artificial intelligence (AI) is a powerful technology that helps cybersecurity teams automate repetitive tasks, accelerate threat detection and response, and improve the accuracy of their actions to strengthen the security posture against various security issues and cyberattacks.[2] This article presents a systematic literature review and a detailed analysis of AI use cases for cybersecurity provisioning. The review resulted in 2395 studies, of which 236 were identified as primary. This article classifies the identified AI use cases based on the NIST cybersecurity framework using a thematic analysis approach.[3] This classification framework will provide readers with a comprehensive overview of the potential of AI to improve cybersecurity in different contexts. The review also identifies future research opportunities in emerging cybersecurity application areas, advanced AI methods, data representation, and the development of new infrastructures for the successful adoption of AI-based cybersecurity in today's era of digital transformation and polycrisis.

This study follows SLR because AI and cyber security field is very large and many research papers are available. Also, this research wants to answer some research questions. SLR is useful because it gives unbiased and scientific

Scopus and Web of Science are popular databases for research papers. In this research, Scopus database is selected because it has more research articles than Web of Science. Scopus also provides better search options and tools to analyze data, so it is easy to use for research work [5]. The search was done between November 2021 and February 2022 to collect research papers related to AI and cyber security. Different keywords related to artificial intelligence and cybersecurity were used. AND and OR operators were used to combine keywords. AI keywords were taken from AI taxonomy and cyber security keywords were taken from NIST framework. After collecting papers, irrelevant studies were removed using inclusion and exclusion criteria.[7] Only important and related papers were selected for this research. At first, 2395 papers were collected from Scopus database. After applying criteria, many papers were removed like non-English papers, reviews, books and duplicate papers. After this step, 2029 papers remained. Then, title and abstract of papers were checked and unrelated papers were removed. After this, 638 papers were selected. After reading full papers, 402 papers were removed. Finally, 236 primary studies were selected for this research and used for analysis and discussion.

They are directly related to the application of Artificial Intelligence in Cyber Security and clearly address the research questions of this study.[8] These studies were further analyzed in detail to understand different AI techniques used, various cyber security domains covered, types of datasets applied, and evaluation methods followed by researchers. By carefully examining these selected studies, this research aims to identify current research trends, commonly used AI approaches, major challenges faced in cyber security, and important research gaps where further improvements or future research can be done.[2] Therefore, these 236 primary studies play a very important role in answering the research questions and achieving the overall objectives of this research work.

While reading all the full papers properly, we realized that many of them were not fully matching our research needs.[2] At first, from title and abstract they looked relevant, but after reading complete paper, it became clear that they were not exactly focused on our topic. AI is an intriguing tool that can provide analytics and intelligence to protect against ever-evolving cyberattacks by swiftly analysing millions of events and tracking a wide variety of cyber threats to anticipate and act in advance of the problem. For this reason, AI is increasingly being integrated into the cybersecurity fabric and used in a variety of use cases to automate security tasks or support the work of human security teams.[7] The flourishing field of cybersecurity and the growing enthusiasm of researchers from both AI and cybersecurity have resulted in numerous studies to solve problems related to the identification, protection, detection, response and recovery from cyberattacks.

Research Methods for Cyber Security teaches scientific methods for generating impactful knowledge, validating theories, and adding critical rigor to the cyber security field.[8] This book shows how to develop a research plan, beginning by starting research with a question, then offers an introduction to the broad range of useful research methods for cyber security research: observational, mathematical, experimental, and applied. Each research method chapter concludes with recommended outlines and suggested templates for submission to peer reviewed venues.[9]

This book concludes with information on cross-cutting issues within cyber security research. Cyber security research contends with numerous unique issues, such as an extremely fast environment evolution, adversarial behaviour and the merging of natural and social science phenomena.[11] Research Methods for Cyber Security addresses these concerns and much more by

teaching readers not only the process of science in the context of cyber security research, but providing assistance in execution of research as well. Presents research methods from a cyber security science perspective Catalyzes the rigorous research necessary to propel the cyber security field forward; Provides a guided method selection for the type of research being conducted, presented in the context of real-world usage [12. Some papers were only slightly connected to Artificial Intelligence and did not actually use AI in solving real cyber security problems. Few studies were mostly theoretical and did not show any practical implementation or experimental results. Some papers did not explain their methodology clearly, and in some cases the results were not properly discussed. [13] There were also studies where the main focus was on improving AI models only, instead of applying AI to solve cyber security issues.

Cybersecurity can be divided into a number of subcategories or types that concentrate on specific facets of safeguarding computer networks, systems, and data. The following are some of the main categories of cybersecurity.[1] Cybersecurity is becoming complex because of the exponential growth of interconnected devices, systems and networks. This is exacerbated by advances in the digital economy and infrastructure, leading to a significant growth of cyberattacks with serious consequences. In addition, researchers report the continued evolution of nation-state-affiliated and criminal adversaries, as well as the increasing sophistication of cyberattacks, which are finding new and invasive ways to target even the savviest of targets [2].

Network Security & Application Security: Network protection requires watching computer networks against interruption, abuse, and attacks.[2] It works to secure network foundation and stop unauthorised approach to sensitive dossiers, to a degree firewalls, interruption discovery and stop systems, in essence private networks (VPNs), and network separation. Application safety is engaging attention insulating software wholes and uses at each stage of happening. In order to find and close protection breach that an attacker takes care of exploit, it requires secure systematised practices, frequent exposure assessments, and seepage experiments.[4] To prevent unauthorised approach to or guidance of programmes, approach controls and authentication processes must more be fixed. Data Security & Cloud Security is protecting data against unauthorised access, disclosure, or change is part of data security [6]. In order to guarantee the security, integrity, and accessibility of sensitive data, this includes putting encryption, access controls, and data loss prevention (DLP) mechanisms into place. Data backup, recovery, and storage protocols are all included in data security. Securing data and applications hosted in cloud settings is the main goal of cloud security.[9] To safeguard cloud-based resources against unauthorised access or data breaches, it entails adopting strong access restrictions, encryption, and monitoring methods. Shared responsibility frameworks and regulations relevant to cloud service providers are also addressed by cloud security. Phishing & Social engineering Phishing is the practice of shipping phoney emails that perform to have reliable beginnings. [10]The objective search out exchange contemplative news like login news and fee card facts. It is the ultimate weighty type of cyberattack. Over education or a mechanics solution that filters injurious electronic mail, you can help protect manually.[12]It is an action secondhand by opponents to deceive you into revealing impressionable news. They can demand a commercial fee or enhance their approach to your private facts. In order to make you more inclined to click on links, spread malware, or support distressing causes, social engineering may be linked accompanying few of the pressures filed above. [14]Cyber threats refer to the potential for a malicious attempt to interfere with or harm a system or computer network. Attacks' objectives vary based on what cybercriminals need. [11]The attacks have an impact on many significant sectors, including the military, financial institutions, governments, enterprises, business, and hospitals that gather, store, and process sensitive computer data and share it with other computers via networks.[15]

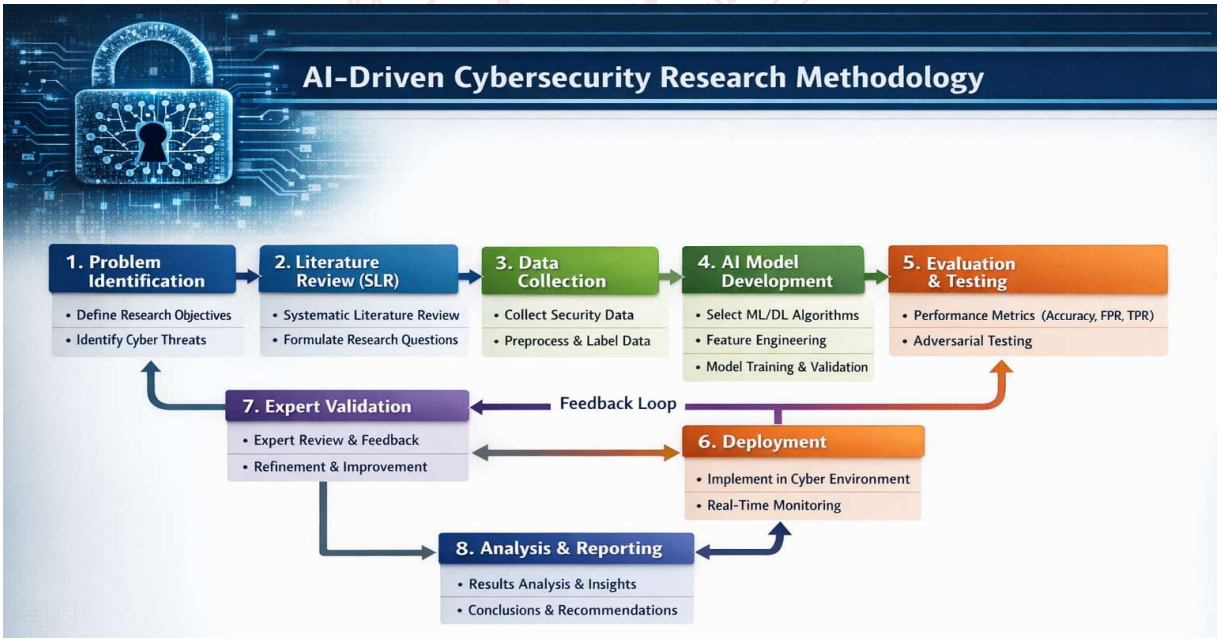


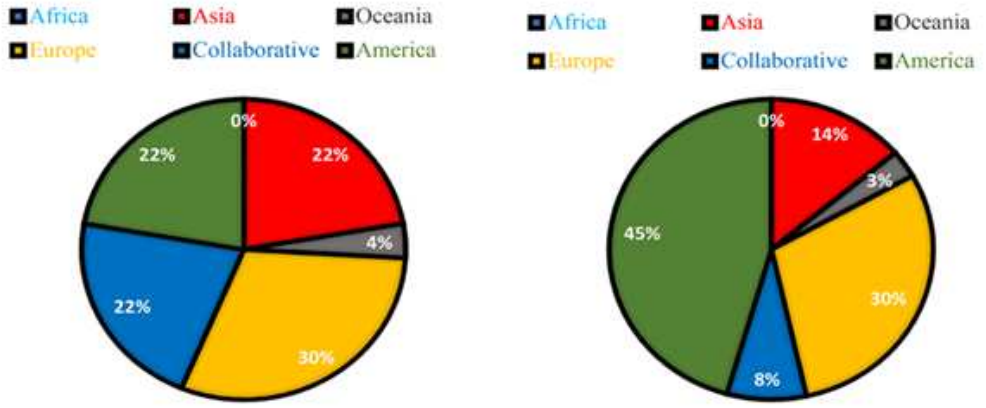
Figure 2: Ai Driven Cybersecurity

4. Result

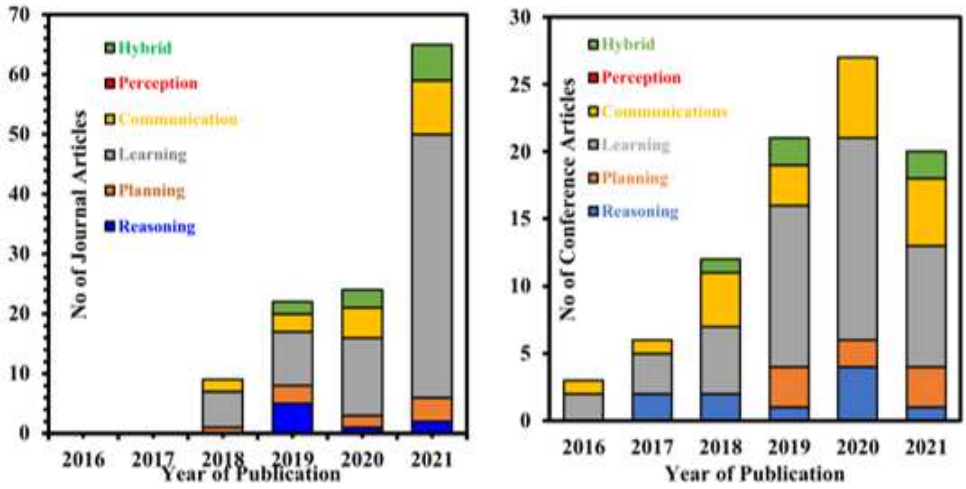
The results of this study are based on the analysis of 236 research papers related to artificial intelligence and cyber security. These papers were studied to understand how AI is used in cyber security functions like identify, protect, detect, respond and recover.

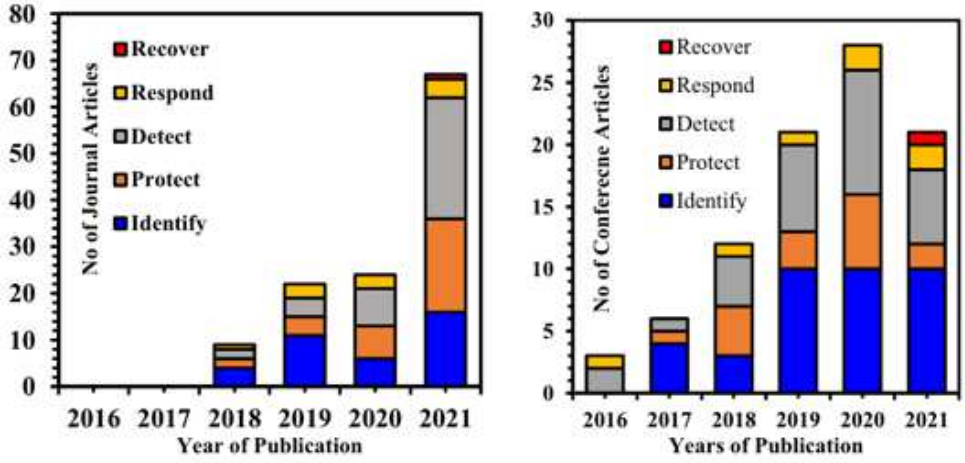
The analysis shows that artificial intelligence is very much used in cyber security for detecting cyber attacks, malware, phishing attacks, hacking and suspicious activities in networks. Many researchers explained that machine learning and neural networks are mostly used AI techniques in cyber security. These techniques help the system to learn from old data and find new and unknown threats automatically.

Overall, the results show that AI plays a very important role in modern cyber security. It improves detection, protection and response to cyber attacks, but still many problems and research gaps are there which need more study in future. This book concludes with information on cross-cutting issues within cyber security research. Cyber security research contends with numerous unique issues, such as an extremely fast environment evolution, adversarial behavior, and the merging of natural and social science phenomena. Research Methods for Cyber Security addresses these concerns and much more by teaching readers not only the process of science in the context of cyber security research, but providing assistance in execution of research as well. Presents research methods from a cyber security science perspective; Catalyzes the rigorous research necessary to propel the cyber security field forward; Provides a guided method selection for the type of research being conducted, presented in the context of real-world usage.



(a). Journal publications (b). Conference publications





5. Conclusion

Artificial intelligence has become an essential part of the information security implementation system. It offers effective critical analysis and efficient threat identification.[11] The study examines the possibilities, aspects, and priorities of using artificial intelligence technologies in the cybersecurity system. It also highlights the benefits and risks of AI in information security. Based on the research outcomes, it was found that artificial intelligence in the field of security canidentify risk priorities, quickly detect malware on the network, direct incident response, and prevent possible attacks before they occur. [12] The study revealed how artificial intelligence systems play a key role in improving information security protocols while eliminating the risks of the human factor. In addition, the authors have identified the dangers and challenges of using artificial intelligence in information security systems.[14] The most significant risks and challenges include the possibility of cybercriminals using the potential of AI and the threat of unauthorized information leakage. The article analyses the main types of AI technologies used in the cybersecurity system. In addition, the authors substantiated the high efficiency of decision support systems using artificial intelligence technologies, as well as risk prevention andsecurity automation.[12] It is obvious that AI can create adaptive security systems that can respond quickly and effectively to changing threats and attacks in real time. At the same time, such systems can automatically adjust security rules and policies to protect networks and data more effectively. [10] Therefore, the combination of artificial intelligence and cybersecurity capabilities opens up the possibility of a paradigm shift in digital security. As a result of the development of such a symbiotic relationship, unprecedented opportunities to counter cyber threats are emerging.[15] The high analytical accuracy of AI technologies, in synergy with their rapid response to new challenges, places them as the driving force behind the forward-looking cybersecurity of the future.

The key concepts associated with artificial intelligence (AI), and thus constituting its domain or space, are those of speed, autonomy, invisibility, action, decision-making, learning, data, etc. [1] With this particular Al space, we must associate its flaws and vulnerabilities, such as errors, biases, imperfections and exposure to attacks, which are the most important aspects of Al

Many of these aspects are already present in the issues addressed by cybersecurity and cyber defense. But when we talk about cyberspace, we are primarily considering reticulation (networking of the world, individuals and societies), and we therefore treat security and defense issues in light of this essential characteristic.[10] The network calls into question the way in which we control space, and therefore the way in which we think about national space, sovereignty, borders, the reduction of distances, power over this space and the militarization of this space.[9] The network highlights the notions of flow, exchange and sharing Cyberspace implies constant fluidity and permanent movement of data, and therefore is a dynamic associated with its own spatialization.

Al is placed at a different level; it calls for other concepts, other ideas, other representations and logies.[2] Nonetheless, it is full-fledged part of cyberspace, without which it is nothing it feeds on data, is made up of applications, acts and circulates in cybermetic space and acts on cybernetic space, which it will modify, disrupt and reconfigure. Introducing new components into cyberspace with different behaviors (intelligent, autonomous, self-adaptive, capable of luring, imitating, blurring the line between true and false, real and artificial) is likely to reshuffle the cards.[12] This evolution is driving an increase in the number, scale and impact of cyberattacks, and necessitating the implementation of intelligence-driven cybersecurity to provide a dynamic defence against evolving cyberattacks and to manage big data. Advisory organizations, such as the National Institute of Standards and Technologies (NIST), are also encouraging the use of more proactive and adaptive approaches by shifting towards real-time assessments, continuous monitoring and data-driven analysis to identify, protect against, detect, respond to, and catalogue cyberattacks to prevent future security incidents [3].

AI is an intriguing tool that can provide analytics and intelligence to protect against ever-evolving cyberattacks by swiftly analysing millions of events and tracking a wide variety of cyber threats to anticipate and act in advance of the problem. [4] For this reason, AI is increasingly being integrated into the cybersecurity fabric and used in a variety of use cases to automate security tasks or support the work of human security teams. The flourishing field of cybersecurity and the growing enthusiasm of researchers from both AI and cybersecurity have resulted in numerous studies to solve problems related to the identification, protection, detection, response and recovery from cyberattacks.[5]

Several reviews on cybersecurity and AI applications were published in recent years [9]. However, to the best of our knowledge, there is no comprehensive review that covers state-of-the-art research to explain cybersecurity activities covered by AI techniques and the details of how they are applied. Therefore, our objective was to provide a systematic review, a comprehensive view of AI use cases in cybersecurity, and a discussion of the research challenges related to the adaptation and use of AI for cybersecurity to serve as a reference for future researchers and practitioners.[11] Table 1 shows a comparison of the study with review articles from recent years.

Reference

[1] She D. et al. “NEUZZ: Efficient Fuzzing with Neural Program Smoothing” 2019

[2] NIST “The NIST Cybersecurity Framework (CSF 2.0) ”2024

[3] NIST “Cybersecurity Framework Profile for Artificial Intelligence” 2025

[4] Wang B. et al. “Skyfire: Data-Driven Seed Generation for Fuzzing” 2017

[5] Godefroid P. et al. “Learn&Fuzz: Machine Learning for Input Fuzzing ”2017

[6] High-Level Expert Group on AI “A Definition of AI: Main Capabilities and Disciplines ”2019

[7] Cummins C. et al. “Compiler Fuzzing through Deep Learning ”2018

[8] Liu X. et al. “DeepFuzz: Automatic Generation of Syntax-Valid C Programs for Fuzz Testing” 2019

[9] Xu H. et al. "DSmith: Compiler Fuzzing through Generative Deep Learning Model with Attention" 2020

[10] Bakirtzis G. et al. "Data-Driven Vulnerability Exploration for Design Phase System Analysis" 2019

[11] Chen Y. et al. "Learning-Guided Network Fuzzing for Testing Cyber-Physical System Defences" 2019

[12] Zhou S. et al. "Autonomous Penetration Testing Based on Improved Deep Q-Network" 2021

[13] Gangupantulu R. et al. "Crown Jewels Analysis Using Reinforcement Learning with Attack Graphs" 2021

[14] Neal C. et al. "Reinforcement Learning Based Penetration Testing of a Microgrid Control Algorithm "2021

[15] Mallick A. et al. "Real-Time Threat Detection Using Hybrid Deep Learning in IoT Networks" 2024

[16] Russo E.R. et al. "Summarizing Vulnerabilities' Descriptions to Support Experts During Assessment"2019

[17] Aota M. et al. "Automation of Vulnerability Classification from its Description Using Machine Learning"2021

[18] Vanamala M. et al. "Topic Modeling and Classification of CVE Database "2020

[19] Achuthan K. et al. "Advancing Cybersecurity and Privacy with AI"Current Trends and Systematic Review 2024

[20] Ferrag M.A. et al. "Generative AI and Large Language Models for Cybersecurity" A Comprehensive Survey 2025