'National Conference on Recent Advances of Computational Intelligence Techniques in Science, Engineering and Technology'
International Journal of Scientific Research in Computer Science, Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

Analysis of Artificial Intelligence Developments and Their Impacts on Cybersecurity

Shammi L[1], Dr. R Senkamalavalli[2], Manimegalai A[1]
[1]Assistant Professor, [2]Associate Professor
Department of Computer Science and Engineering, East Point College of Engineering and Technology, Karnataka, India

ABSTRACT
Artificial Intelligence (AI) is a potent tool that cybersecurity teams may use to automate repetitive processes, speed up threat detection and response, and increase the efficacy of their actions to fortify the security posture against a variety of security problems and cyberattacks. According to experts, Machine Learning (ML) and artificial intelligence both have beneficial and harmful consequences on cybersecurity. AI algorithms learn how to react to various scenarios using training data. They pick up new information by replicating and supplementing it along the way. This article examines AI's effects on cybersecurity, which are beneficial as well as detrimental.

Keywords: Cybersecurity, AI, Cyber threats, Artificial Intelligence, Machine Learning

I. INTRODUCTION

Networks, devices, Programmes, and data are protected by networks, processes, and practices known as cybersecurity from intrusions, damage, and unauthorized access. "Cybersecurity refers to the set of activities and measures, both technical and non-technical, intended to protect the 'real geography' of cyberspace as well as devices, software, and the information they contain communicated, from all possible threats," according to the definition given by Myriam Dunn Cavelty [3]. One of the most crucial challenges in cyberspace nowadays is cybersecurity [4, 5].

The 20th century saw the development of artificial intelligence. In an effort to design a structure that wouldn't need a human brain's assistance, this development came about. More research was done on the subject as a result of the discovery. Robot and intelligent system development have increased. The advances all made an effort to integrate a piece of technology that acts like a person but mimics human behaviour. Numerous mathematicians attempted to create formulas to aid with the element of the research, which also included mathematics. AI platforms assist enterprises in the development, management, and deployment of machine learning and deep learning models at scale. Decreasing software development tasks such as data management and deployment make AI technology more accessible and economical [2]. With the increase in cyber risks, artificial intelligence (AI) is increasingly widely employed to monitor and restrict cybercrime.

II. OVERVIEW OF ARTIFICIAL INTELLIGENCE

AI platforms let businesses create, manage, and deploy machine learning and deep learning models at scale. As businesses compete to incorporate AI technology into their goods, business strategies, or security programmes, the impact of AI on cybersecurity is swiftly growing in importance. The topic of artificial intelligence is increasingly becoming one that has the potential to revolutionize cybersecurity. However, the use of AI to cybersecurity poses fresh problems and hazards in addition to offering fresh and creative solutions. In order to employ AI in cybersecurity responsibly and ethically, it is crucial to grasp both its potential and its limitations.
AI technologies can understand, learn, and act based on the information derived from events and effects. According to Stuart Russell and Peter Norvig, "AI attempts not just to understand but also to build intelligent entities" and they offered a definition for AI, organized into two main categories, such as:

- thought process and reasoning: these measure success in terms of thinking, which is categorized into thinking humanly and thinking rationally.
- behavior: this measures a success based on the ideal performance and action, and it is categorized into acting humanly and acting rationally.

AI works in three ways [2]:

- Assisted intelligence, which improves what people are already doing
- Augmented intelligence, which empowers people to do things that they could not do
- Autonomous intelligence, which are features of machines that act on their own.

With respect to these three categories, it could be concluded that AI aims to solve some of the most difficult problems and cybersecurity falls into this category, since cyberattacks have become highly sophisticated and potentially more disastrous and turned to be a complex issue in cyberspace.

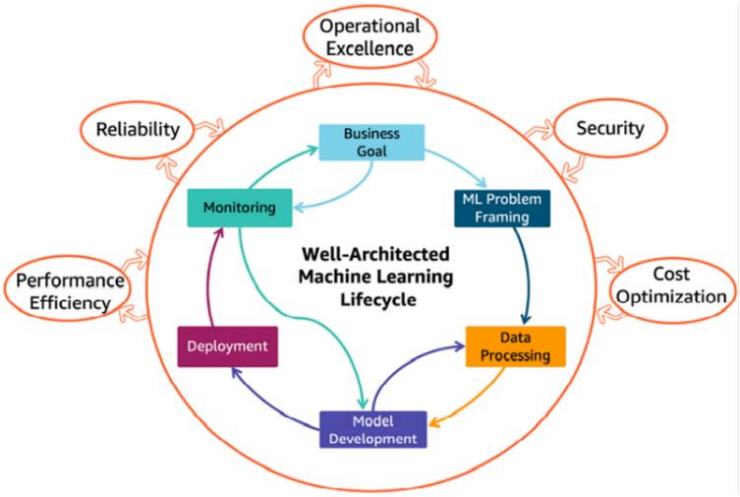

Fig:1 Machine Learning Life Cycle [4]

The greatest serious threat to corporations, organisations, and governments around the world is cyberattacks, which are continually being fought against by cyber security and intelligence firms globally. Cyberattacks are growing more frequent and effective as technology advances and makes life easier and more convenient every day. The huge arsenals that cybercriminals and malevolent third parties possess enable them to launch large-scale attacks.

III. AI CONTRIBUTION IN CYBERSECURITY

Artificial Intelligence has many applications in different sectors and industries. One of the sectors that have continued to benefit from artificial intelligence has been cybersecurity. In order to better understand the notion of various applications of AI for cybersecurity, this section analyses the background data pertaining to the core topics of this review, including the operational definition of cybersecurity and the AI taxonomy.

One of the many applications for artificial intelligence is cybersecurity. According to a Norton research, the average data breach recovery costs $3.86 million globally. According to the survey, it takes businesses 196 days on average to recover from a data breach. Organisations should increase their AI spending in order to prevent time wastage and financial losses. In data security measures and protocols, AI technology has been one of the best technologies in ensuring that they have improved them. Data is critical to business organizations, so it needs to be secured [6]. With the help of multiple data encryption protocols, the system can facilitate great encryption and guarantee the security of the data involved. The great protocol significantly impacts the technology in the cybersecurity sector of technology [2].

Threat intelligence, AI, and machine learning can identify trends in data to help security systems learn from the past. Additionally, AI and machine learning help businesses adhere to security best practises and speed up incident reaction times. In order to safeguard information and communication systems and the data they contain from harm, unauthorised use or modification, or exploitation, cybersecurity policies, procedures, and technical measures are put in place. The problem is made more difficult by the quickening rate of technological advancement and innovation as well as the rapidly changing nature of cyber threats. AI-based cybersecurity tools have evolved to assist security teams in effectively reducing risks and enhancing security in response to this unprecedented challenge. A generally acknowledged and streamlined taxonomy is required to review the research on using AI for cybersecurity due to the heterogeneity of AI and cybersecurity. Threats are recognised using signatures or indicators of compromise in traditional security procedures. This method may be successful against threats that have already been experienced, but it is ineffective against threats that have not yet been identified.

About 90% of threats [1] may be detected using signature-based strategies. Artificial intelligence (AI) can improve detection rates up to 95%, however there will be a huge number of false positives. The best course of action would be to use both conventional techniques and AI. By doing this, false positives can be reduced and the detection rate can reach 100%. Businesses can also utilise behavioural analysis in conjunction with AI to improve the threat hunting process. By processing large amounts of endpoint data, for instance, you can use AI models to create profiles of each application within a network for an organisation.

Fraud Prevention Techniques Using Artificial Intelligence: Fraud attempts and breaches are more nuanced, with organized crime and state-sponsored groups using machine learning algorithms to find new ways to defraud digital businesses.[9]. Fraud-based attacks have a completely different pattern, sequence, and structure, which make them undetectable using rules-based logic and predictive models alone.

The future of AI-based fraud prevention relies on the combination of supervised and unsupervised machine learning. Supervised machine learning excels at examining events, factors, and trends from the past. Historical data trains supervised machine learning models to find patterns not discernible with rules or predictive analytics. Unsupervised machine learning is adept at finding anomalies, interrelationships, and valid links

between emerging factors and variables. Combining both unsupervised and supervised machine learning defines the future of AI-based fraud prevention and is the foundation of the top nine ways AI prevents fraud:

- AI is re-defining fraud prevention from relying only on past experiences to taking into account emerging activities, behaviors, and trends in transaction anomalies. By combining supervised learning algorithms trained on historical data with unsupervised learning, digital businesses gain a greater level of acuity and clarity about the relative risk of customers' behaviors.
- **AI makes it possible to detect fraud attacks in real-time versus having to wait six or eight weeks until chargebacks start coming in.** By balancing supervised and unsupervised learning, AI alleviates the need always to play catch-up to online fraud.
- By having an AI-based fraud prevention system do the work of evaluating historical data and anomalies, customer experiences can stay more positive, and the more sophisticated nuanced abuse attacks can be stopped.
- **Provides fraud analysts with real-time risk scores and greater insight into where best to set threshold scores to maximize sales and minimize fraud losses.** Adding in anomaly detection and insights into real-time activity using unsupervised machine learning, fraud analysts can instantly validate or redefine their decision regarding threshold levels, managing risk well.
- **AI enables digital businesses to gain greater control over chargeback rates, decline rates, and operational costs so that business objectives can be achieved.** Digital businesses are relying on the combination of supervised and unsupervised machine learning to attain greater levels of agility, speed, and time-to-market, with AI-based fraud prevention systems being foundational to that effort.
- **Enables digital businesses selling virtual goods, including gaming, to provide a more consistent, high-quality user experience on a 24/7 basis**. AI makes it possible for gamers to buy the coins or tokens they need when they need them to keep playing. AI-based fraud prevention systems make it possible to immediately accept the transactions while still staying within the chargeback thresholds from American Express, MasterCard, VISA, and others.
- **AI reduces the friction customers experience by helping merchants easily approve online purchases and reduce false positives.** AI-based fraud scores like Omniscore reduces false positives, which is a major source of friction with customers. All this translates into fewer manual escalations, declines, and an overall more positive customer experience.
- **Staying in compliance with internal business policies, those from regulatory agencies and agreements with distribution partners is where AI-based fraud prevention is contributing today**. AI-based scoring and fraud prevention are extensively used to keep businesses in compliance.
- **Enables low-margin businesses and product lines to stay profitable by controlling chargebacks levels that have a direct impact on margins.** AI-based approach that incorporates both unsupervised and supervised learning pays off from a gross margin standpoint.

Mengidis et al. [2] also state that including artificial intelligence learning systems in cybersecurity helps prevent attacks in a system. The learning-based system learns from the attackers' actions ad adjusts to protect the information. This factor makes it impossible for attackers to gain access to the data. Having a system that keeps adjusting and learning is one of the attributes that has made the technology very efficient. AI has been able to avoid cyber-attacks using the approaches discussed below. The different techniques ensure the efficiency of AI in cybersecurity.

Applications of AI in Cybersecurity

A. Signature Based Techniques

Signature intrusion detection systems (SIDS) use pattern matching techniques to detect a known attack; these are also referred to as Knowledge-based Detection or Misuse Detection. 6 Matching methods are used in SIDS to locate a previous intrusion triggering an alarm signal whenever an intrusion signature matches one from a previous intrusion existing in the signature database. The most well-known SIDS currently available are Snort, Suricata, NetSTAT and Bro. The method involves AI detecting cyberattacks and malware through the available codes [9]. The database where malware signatures are stored, is called the blacklist. The system detects the attack by comparing the available signatures in the blacklists to the known signature caught in the attack. The signatures are sometimes referred to as the patterns present in the attack, and this could be said to be another form of machine-based learning [3]. Although the method has proven very efficient over the years, it has been seen to be useless in the case of a new attack. The technique fails since the database has no record of the attack [1]. Changing their patterns ensures they can access the data and information before they are detected.

B. Machine Learning

Mengidis et al. [1] discovered that humans always make mistakes when analyzing data or information. The AI technology detects systems, analyses the available records, and detects logs included in the system. This factor ensures that system administrators can change the information accessed to avoid further loss. This factor has led to the analogy that AI closely replaces human analysts. Classification and clustering are great attributes of machine learning systems [8]. They compare the available information and how it should be in the logs. This factor provides detection if there are errors in the system. The regular records are compared to the current ones to identify the infected logs. After an attack has been detected, necessary steps are taken to ensure the attack has been stopped. Clustering involves grouping the available records or information from the system and detecting anomalies. Both of these techniques used in machine learning have proven effective since it is impossible for humans.

C. Network Intrusion Detection

Network attacks are one of cyber security's most used forms of aggression. The raids are conducted through the networks that the organizations or companies use. It is always important to detect attacks through networks. This factor gives the system the advantage of stopping the attack from the web. Stopping attacks from the web is the first step in protecting the information available. This approach has thus been very efficient in preventing

future attacks [9]. The main key attribute and advantage of network intrusion detection systems are that they have five elements that support the full security of such networks. The first key element is how AI systems acquire large sums of information from the network. This factor can be achieved through the AI system's ability to analyze large amounts of data [3]. All the factors help ensure the security of the network has been completed. Stopping an attack from the network gives the organization a higher chance of protecting the information. All the way a network may be compromised is avoided using the AI techniques available.

D. Phishing Attacks

Phishing attack involves some type of social engineering where the attacker sends fraudulent messages tricking the victim into providing his credentials [4]. Attackers could also engage in a mass phishing attack which targets a group of people to directly impact the vulnerable individuals [7]. AI-based Cybersecurity awareness training should therefore be adopted by more organizations, thus reducing the number of global phishing attacks.

The market for artificial intelligence in cybersecurity is also anticipated to grow during the forecast period as a result of the proliferation of 5G technology [5] and the rising demand for cloud-based security solutions among small and medium-sized organizations. In order to secure information, artificial intelligence in cybersecurity is gradually gaining prominence. The market for artificial intelligence in cybersecurity is continuously expanding because end users are anticipated to adopt AI in cybersecurity to solve security problems and recognise new forms of assaults that can occur at any time.

IV. AI CONTRIBUTION IN CYBERSECURITY

While enhancing security, artificial intelligence and machine learning can make it simpler for hackers to break into networks without human assistance. This has the potential to seriously harm any business. In order to want to minimise damages and maintain the viability of a company, getting some sort of security against cybercriminals is of the utmost importance. AI concerns for cybersecurity, as well as advanced tools to thwart attack.

Intelligent attacks

1. **AI-driven malware:** Artificially intelligent malware. In the hands of hackers, AI-driven malware can infect devices faster than ever before, becoming harder to detect, targeting more victims and creating more convincing phishing attacks. [4]
2. **Vulnerable applications:** Weak application security creates an entry point for hackers to infiltrate. Cybercriminals use AI to hide malicious codes within applications, sometimes programming the attack to execute well after the app has been installed. Malicious codes can be present for years before they strike.
3. **Expanded attack surface:** Through hybrid work, employees are spread across distant locations and often access the cloud on their personal devices. This widens the surface area for cyberattack. AI creates an even more evolved threat landscape, expanding what devices and machines can be used to infiltrate systems.

4. **Constant evolution:** Artificial intelligence is always evolving. While the benefits include enhanced threat detection, there are two sides to that coin. Cybercriminals are constantly learning from existing AI tools to develop more advanced attacks and improve their malware. Security must constantly evolve as well.

The use of AI technology has a wide range of effects across numerous industries. These effects cover both this technology's advantages and drawbacks. It is evident from the explanation above that the advantages of AI for cyber security outweigh any drawbacks. More study is being done on artificial intelligence as it continues to develop. This aspect demonstrates the significant technological developments being made in the methods employed to guarantee cybersecurity support. The practises demonstrate the technological influence of cybersecurity measures. The research mentioned above also focuses on various AI-related cyber security limitations. The boundaries demonstrate how individuals have been able to exploit AI to their advantage. This element has caused cybersecurity to be constrained.

V. CONCLUSION

AI and machine learning are redefining every aspect of cybersecurity today. From improving organizations' ability to anticipate and thwart breaches, protecting the proliferating number of threat surfaces with Zero Trust Security frameworks to making passwords obsolete, AI and machine learning are essential to securing the perimeters of any business. Rapid growth of cyber threats and sophistication of cyberattacks require new, more robust, flexible, and scalable methods. In current research, the main targets of AI-based algorithms for cybersecurity are malware detection, network intrusion detection, and phishing and spam detection. Various researches leveraged a combination of different AI techniques, such as ML/DL methods together with bioinspired computation, or different learning methods such as supervised learning together with reinforcement learning. Although the role of AI in solving cyberspace issues is inevitable, some problems related to trust to AI and AI-based threats and attacks would be another concern in cyber environment.

VI. REFERENCES

[1]. Meeraj Farheen Ansari, Bibhu Dash, Pawankumar Sharma, Nikhitha Yathiraju, "The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review:" Vol. 11, Issue 9, September 2022 DOI: 10.17148/IJARCCE.2022.11912.

[2]. P. Panagiotou, N. Mengidis, et al., Thodora Tsikrika, Stefanos Vrochidis, Ioannis Kompatsiaris, "Host-based Intrusion Detection Using Signature-based and AI-driven Anomaly Detection Methods", Vol. 50, no. 1 (2021): 37-48, ISSN 1314-2119(online).

[3]. Areej Fatima, Tahir Abbas Khan, Tamer Mohamed Abdellatif, Sidra Zulfiqar, Muhammed Asif, Waseem, "Impact and Research Challenges of Penetrating Testing and Vulnerability Assessment on Network Threat", 2023 International Conference on Business Analytics for Technology and Security (ICBATS), Dubai, United Arab Emirates, 2023, pp. 1-8, DOI: 10.1109/ICBATS57792.2023.10111168.

[4]. Katanosh Morovat, Brajendra Panda, "A Survey of Artificial Intelligence in Cybersecurity", 2020 International Conference on Computational Science and Computational Intelligence (CSCI), DOI: 10.1109/CSCI5 1800.2020.00026.

[5]. Meraj Farheen Ansari, Pawan Kumar Sharma, Bibhu Dash, "Prevention of Phishing Attacks Using AI-Based Cybersecurity Awareness Training", International Journal of Smart Sensor and Adhoc Network", Vol 3, Issue 6, March 2022.

[6]. Rammanohar Das and Raghav Sandhane, "Artificial Intelligence in Cybersecurity", ICACSE 2020, Journal of Physics: Conference Series, 1964(2021)042072, DOI: 10.1088/1742-6596/1964/4/042072.

[7]. Zhibo Zhang, Hussam Al Hamadi, Ernesto Damiani, Chan Yeob Yeun, And Fatma Taher, "Explainable Artificial Intelligence Applications in Cyber Security: State-of-the Art in Research", 5th September 2022, IEEE Access, DOI: 10.1109/ACCESS.2022.3204051.

[8]. Navid Ali Khan, Noor Zaman Jhanjhi, Sarfraz Brohi, "Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic", TechRxiv Powered by IEEE – 2020, DOI: 10.3622/techrxiv. 1227879.v1, researchgate.net.

[9]. Bibhu Das, Meraj Farheen Ansari, Pawankumar Sharma, Azad Ali, "Threats and Opportunities with AI-Based Cyber Security Intrusion Detection: A Review", International Journal of Software Engineering and Applications, Vol.13, No. 5, September 2022.