World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

The implications of Artificial Intelligence (AI) on cybersecurity: A detailed review for multidomain industry

Avaneesh Mohapatra * and Gagan Reddy

West Forsyth High School, Cumming, Georgia, United States of America.

World Journal of Advanced Research and Reviews, 2024, 23(02), 1926–1937

Publication history: Received on 07 July 2024; revised on 19 August 2024; accepted on 21 August 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.23.2.2480

Abstract

Cyber threats are becoming increasingly complicated and diverse, posing serious risks to individuals, businesses, and organizations in the cybersecurity sector. The cybersecurity industry needs to change to combat these new dangers as cybercriminals are always coming up with new ways to get past protections. This paper investigates how artificial intelligence (AI) may both simplify and improve cybersecurity efforts. AI has transformed the industry by offering cutting-edge defensive technologies, but it also gives cybercriminals new tools at their disposal to automate and enhance their hacking methods. The effect of AI on authentication procedures—which are crucial for protecting network access—is given special attention. This paper emphasizes the critical need for creative remedies to defend against more complex cyberattacks by examining the dual nature of AI in cybersecurity.

Keywords: AI; Cybersecurity; Social Hacking; Ethical hacking; AI-driven cyber intelligence

1. Introduction

Cybersecurity is an ever evolving and fascinating field that tackles the biggest threat to businesses, organizations, and everyday people in the contemporary world. Cyberthreats have become incredibly complex and multifaceted in nature and become very difficult to respond to (Mohammed et. al, 2024). Cybercrimes can endanger businesses' reputations, financial losses, and individuals. Cybercriminals are constantly searching for new ways to penetrate defense mechanisms for data breaches and fraud to turn commonplace. As time continues, we see new attacks in the forms of malware, viruses, ransomware, and bots to name a few. However, the field of cybersecurity and the threats of cyberattacks have begun to become much more pervasive and lethal through the influence of artificial intelligence (AI) (Dash & Sharma, 2023). Artificial intelligence, or the mimicry of human intelligence done by machines, has played a vital role in revolutionizing various industries, one of the most notable being cybersecurity. AI gives cybercriminals many new ways to improve their methods of hacking and breaching. This can be seen through the way that AI allows the automation and generation needed to bypass certain defenses put in place by cybersecurity engineers. AI can specifically be seen as an issue when looking into the authentication aspect of cybersecurity in which organizations are to keep their networks secure by permitting only authenticated users or processes access to protected resources. AI allows methods in which a cybercriminal can mimic the functions of a human through many biometric features like voice or looks to bypass the authentication software put into place. There are also many issues presented with banking and financial institutions, mainly focusing on the issues presented with the faking of another person's identity, through the usage of AI. This issue requires an understanding of the practices that AI utilizes to mimic humans, in order to differentiate the actions of a real human and a machine attempting to impersonate one. Therefore, cybersecurity and its implications on contemporary society can be greatly improved, while financial losses, losses to business reputations, people taking advantage of weak cybersecurity system architectures, , damages to national security, losses in healthcare, and innocent people losing money can be prevented.

* Corresponding author: Avaneesh Mohapatra

1.1 History of Cybersecurity

The history of cybersecurity spans back to the 1960s, as the concept of cybersecurity began to take shape as mainframe computers and early networks were developed. In the 1960s, computers were costly; only governments, universities, and large companies possessed them. These early computers were still far from what we know today as “Computers in the '60s were large and immobile and in order to make use of information stored in any one computer, one had to either travel to the site of the computer or have magnetic computer tapes sent through the conventional postal system.” (A Brief History of the Internet). Afterward, the United States Department of Justice created the ARPANET, a predecessor to the Internet.

1.2 The Network Control Program

The Network Control Program (NCP) was designed to manage host-to-host communication and facilitate the initial instructions, such as Telnet and File Transfer Protocol (FTP). Its communication method would be packet-switching technology. In order to transfer messages across hosts, an Interface Message Processor was created. This is regarded as the original router or packet gateway. Hardware modems were created and sent to the different organizations.

1.3 The First Virus

In 1971, Bob Thomas of BBN developed the Creeper software, which is frequently recognized as the first virus. This virus was effective at the time as “This virus was able to connect to the network using the modem and to send the copy of itself to the remote computer.” (Mukayeva, 2011). Over the ARPANET, Creeper left behind the message, "I'm the creeper: Catch me if you can," as it passed across Tenex terminals. Ray Tomlinson—the man who created email—was drawn to the Creeper software. Tomlinson changed the code so that it could replicate itself. This made Creeper the first computer worm. In 1972, “after Tomlinson created the world’s first computer worm, he developed the first antivirus program. Tomlinson called this program ‘Reaper.’ It was developed specifically to remove the Creeper program and it succeeded” (Gcu, 2019). Eventually in 1977, “the US standards body NBS (National Bureau of Standards) — now renamed NIST (National Institute of Standards and Technology) — identified a need for a government-wide standard for encrypting unclassified, sensitive information”(idk). This gave birth to the Data Encryption Standard (DES).

1.4 The DES

The DES was adopted as a federal standard for encrypting electronic data. The 1980s were known as the rise of personal computing and malware. In the early 1980s, the term "computer virus" came about as, “In 1984, mathematician Dr.Frederick Cohen introduced this term, thereby becoming the “father” of computer viruses with his early studies of them“(Szor, 2005)when he did a study on the topic. In 1986, the first PC virus, "Brain," was created by two Pakistani brothers, initially intended to protect their medical software from piracy. In 1988, the Morris Worm, one of the first widespread worms, was released, causing significant disruption and highlighting the need for better network security.

1.5 The First Web Browser

Eventually, in 1992, the first web browser, Mosaic, was released, making the internet more accessible to the public and increasing the potential for cyber threats. “The first macro virus discovered in 1995 was WM Concept, which was drafted in Microsoft Word macro language” (Alenezi et al, 2020). The first DDoS attack was launched in 1999 “using a tool called Trinoo. It targeted a computer in University of Minnesota through at least 227 bots” (Bekshentayeva, 2015). Due to these increased cyberattacks, the early 2000s saw a similar issue. The ILOVEYOU virus was a virus that went through e-mail systems and had the subject line “ILOVEYOU” and an attachment file labeled “LOVE-LETTER-FOR-YOU.TXT.vbs.” This email drew the attention of numerous people due to curiosity. “Within a few hours a 100,000 systems had been infected; by the end of the week when the epidemic had begun to subside, the virus had struck 45 million computers in 20 countries, causing an estimated $8 billion in damage” (Knight, 2000).

As technology continued to evolve, AI and other more advanced bots made way for new viruses, phishing attacks, and data obstruction. T o prevent these issues and threats, new and improved security was implemented causing cybersecurity to be more secure than ever. Still, there are ethical concerns about the effects of AI and other ways to manipulate data despite these strong cyber protection programs. These foundational developments laid the groundwork for the complex and sophisticated field of cybersecurity that continues to evolve today. This calls into question how cybersecurity programs can be improved using tools such as AI and other programs.

2 History of Cybersecurity

Table 1 F1: The table shows major cyberattacks throughout history and why they are important to the evolution of cybersecurity.

Year	Event	Why It Was Important
1988	Morris Worm	One of the first widespread internet worms, highlighting vulnerabilities in networked systems.
2000	ILOVEYOU Virus	A widespread email virus that caused billions in damage and demonstrated the destructive potential of social engineering.
2003-2006	Titan Rain	Series of coordinated attacks allegedly by Chinese hackers targeting U.S. defense contractors, emphasizing the rise of state-sponsored cyber espionage.
2010	Stuxnet	A sophisticated worm that targeted Iranian nuclear facilities, showing the potential of cyber weapons to impact physical infrastructure.
2014	Sony Pictures Hack	A major breach attributed to North Korean hackers, resulting in leaked sensitive data and highlighting the vulnerabilities of corporate networks.
2015	Anthem Breach	Exposed personal information of nearly 80 million people, stressing the critical need for robust cybersecurity in healthcare.
2015	Ukrainian Power Grid Attack	The first known successful cyberattack on a power grid, demonstrating the vulnerabilities of critical infrastructure.
2017	Equifax Breach	Exposed personal data of 147 million people, illustrating the severe impact of data breaches on individuals and organizations.
2017	WannaCry Ransomware	A global ransomware attack that disrupted numerous organizations, underscoring the need for updated security measures and preparedness against ransomware.

3 Business Reputations

Cybersecurity is a major sector of many businesses through its role in creating safe user authentication, protecting high-value assets, and lowering the risk of any exposure to sensitive data or information. Businesses often have critical data that would hurt them if it were ever released; this is known as a high-risk asset. Authentication ensures that only authorized individuals or users can view and access limited resources and information to limit the spread of data which can help prevent leaks from occurring. The introduction of AI brings about many issues to the current authentication systems commonly utilized by businesses.

3.1 AI in Deepfakes

AI-powered cyberattacks use AI or machine learning (ML) algorithms and methods to automate and enhance the many current phases of a cyberattack. AI is used to identify vulnerabilities, implement operations along identified vectors, interfere with system operations, and manipulate data. One of the most notable of these is the way that AI allows users to create fake videos and audio that mimic higher-up executives in the company. This type of vulnerability leads to potentially bypassing defenses and allowing access to sensitive data, while also harming the public perception of the individual and overall company.

Figure 1 Image showing how AI are able to mimic human behavior and bypass biometric security standards.

3.2 AI in Social Hacking

Forms of social hacking are another platform in which AI can be utilized to access company information. AI can train off of social data from emails, media, and conversations to create its own emails that are human-like and more likely to be accessed by a current employee of the company. Moreover, these types of AI-powered attacks can be automated. This is important as, "However, growing access to AI- and generative AI-enabled tools is allowing adversaries to automate attack research and execution".(Stanham, 2024). This makes these attacks much more common and viable for cybercriminals to attempt. When these types of incidents occur within businesses, their reputation becomes slandered and defamed through customer trust and public perception.

Figure 2 Image showing how through Ai powered social hacking, malicious emails can be sent and received

3.3 Real world example

This type of Cyber-attack can be seen recently in a real-world setting through the data breach that happened to Capital One in which, "On July 19, 2019, we determined that an outside individual gained unauthorized access and obtained certain types of personal information from Capital One credit card customers and individuals (…)." (Neto et al. , 2020). With Capital One being the 5th largest consumer bank in the U.S. at the time, many people rely on it to keep all of their credentials and information safe. However, when cyber-attacks can be performed effectively as seen in this case, and especially if they were to be made more common through AI, many people are placed at risk when relying on the current

cybersecurity system architectures. Therefore, cybersecurity plays a crucial role in businesses by guaranteeing secure user authentication, protecting valuable assets, and reducing the likelihood of sensitive data getting leaked. Strong authentication procedures are essential for limiting access to only those who are authorized and avoiding data breaches.

4 Ethics of Cyberattacks

From many people's perspectives, machine automation is seen as a tool that can help them with many aspects and avenues of their lives. The bounds of automation are something that is constantly being explored and utilized in many different fields. However, automation is commonly used for unethical pursuits of personal benefits when it is able to bypass current cybersecurity systems. Some of machine automation's, most serviceable qualities are in its capability to act like a human while still avoiding detection from the newest cyber defenses. While many new forms of cybersecurity defense measures are constantly being innovated and improved upon, Automated bots can still avoid its detection through their capacity to adapt in real time and learn to avoid.

4.1 Automated Engagement

Another form of this is in manipulating engagement metrics through the use of automotive features. People use automated machines to constantly send unsolicited communication in bulk (commonly known as spam) with different engagement metrics such as clicks or fake interactions that boost their platform and profile and ultimately spread their reach to a larger amount of people around the world. Through all these different forms of growing their reach and influence, the result is a vast amount of money brought in through sponsorships and brand deals that individuals don't deserve due to their unethical way to fame. This creates a way for people to abuse the intelligent and practical nature of machine automation to gain money and fame. This issue is also made more common as not only are these bots often found at cheaper prices with easy access, but also many smaller streamers who don't have much to lose are willing to take the risk of being caught. This is illustrated by "The 2018 annual report of Distil Networks [2] reveals that web bots account for 42.2% of all website traffic while human traffic makes up the rest 57.8%. (Xu et al.). This means that nearly half of all data is completely wasted, and any marketing and advertising teams attempting to reach people are effectively wasted due to people faking their view counts and filling their own pockets.

Figure 3 Image illustrates how Automated machines are able to bypass securitys at large scales.

4.2 Automation on Public Opinion

Another unethical side to the usage of these automated machines is when the usage is intended to sway public opinion and have harmful effects. This automation of followers/likes allows the mass production of inputs on social media and polls to spread a great amount of disinformation over a topic to the common person, whether that be propaganda or fake news. This is illustrated from "The 2018 study's authors estimated that bots on Twitter created two-thirds of Twitter links to popular sites" (Smith, 2024, 419).

4.3 Automation on Politics

Another form of this can be seen in a political context where people may want to sway their opinions toward a candidate or side they greatly favor. This allows them to be able to make great influence over an election without having to work to amass a big platform. This is also seen in the real-world in a study of 2016 election-related tweets, "Among the findings were that social bots generated spikes of conversations around real-world political events" (Smith, 2024, 422). This was also while increasing the consumption of content by those who shared their political views

This shows that, even though computer automation has numerous advantages, its technology is frequently abused for unethical purposes. It has the ability to automate actions that control online interaction, including sending spam to increase metrics or buying views and followers. Automation can avoid detection due to its versatility, even with the progress made in cybersecurity. To guarantee the appropriate use of Automation, these problems must be resolved.

5 Financial attacks on financial systems

One of cybersecurity's biggest applications can be found in the finance industry. Throughout many different financial institutions such as insurance companies, credit unions, and variations of banks cybersecurity is commonly relied on. Cybersecurity is used to protect sensitive client data, stop identity fraud, authenticate users, and have real-time monitoring of the various functions that occur. AI introduces various new forms of cyberattacks that become implemented against these establishments. All of these new attacks have the benefit of AI's ability to automate many different manual processes, adaptive learning, and mass production. Through these new features, financial institutions are put at a big loss by trying to keep up their cyber defense against incoming threats while also mitigating any damages that are being caused.

5.1 Artificial Identity Fraud

One of the most notorious forms of these AI-driven cyber threats is the emergence of artificial identity fraud, in which the criminal uses AI to create a highly realistic identity in order to pursue fraudulent actions without any detection. This is easily made possible due to the fact that AI is able to study and learn from data on people's profiles and features that it can then replicate to complete said actions. This identity fraud then leads to the financial institution losing money and capital from fake accounts and transfers.

5.2 AI in DDoS Attacks

Another form of attack is through direct attacks on the networks such as a distributed denial-of-service(DDoS). In these attacks, cybercriminals attempt to disrupt the network through an overload of packets being sent in, faster than the server can handle at once. This is then made highly effective through the improvement in coordination and production that is offered with AI, thus resulting in significant server outages for users and even more costs for recovery and improvement.

5.3 AI on Financial Markets

Another way that AI can be utilized is in the trading market. AI systems can manipulate and influence markets by conducting trades at high frequencies, causing market discrepancies. These actions are also based on real-time learning of the market conditions and data that allows it to be accurate and profitable for the user. This causes there to be great instability in financial markets while also harboring great financial loss for those affected. Furthermore, any type of cyber threat is made much more potent through the fact that AI is able to scan for any vulnerabilities or weaknesses within a network at a large scale, allowing for the exploitation of those weaknesses to be made easier. During this action, the AI is also capable of adapting to new defenses, permitting it to constantly analyze networks. This is illustrated by the fact that "In 2023, IC3 received a record number of complaints from the American public: 880,418 complaints were registered, with potential losses exceeding $12.5 billion" (Federal Bureau of Investigation, 2023). As criminals begin to get hold of more and more AI tools, they are able to outdo federal banks more and more, resulting in this sudden increase in financial losses being experienced by financial institutions worldwide.

5.4 Systematic Financial Affect

With the rise of these various issues becoming more and more prominent throughout many places, a systematic financial disruption could arise. As more and more failures between institutions amass, we could see huge parts of the industry affected. As people start to harbor distrust towards their personally used institutions, they may start drawing back and spreading the word. Thus leading to real negative effects throughout the entire sector and economy. This is displayed in "Lloyd's of London report forecasts 'a cyber incident that takes a top three cloud provider offline in the US

for 3–6 days would result in ground-up loss central estimates between US$6.9 billion and US $14.7 billion' "(Warren et al, 2018). This issue of great loss impacting a large part of a sector is made even worse due to the fact that many of these institutions are often interlinked. This means that as one of these institutions is impacted, they hold the risk of another being consequently harmed, thus leaving huge impressions upon the sector and economy as a whole.

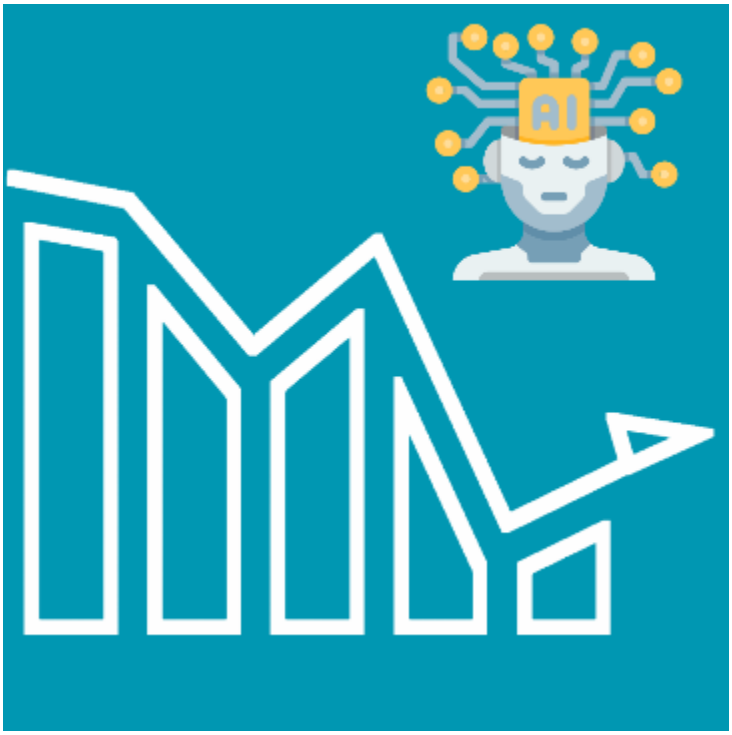

Figure 4 Image showing how financial institutions and sectors are gradually losing capital from AI-powered Cyberattacks

6 National Security & Infrastructure

The increasing prevalence of cybersecurity attacks on national security has created serious risks to nations across the globe. Artificial Intelligence (AI) has led to a further evolution in the cyber threat landscape, presenting new security issues as well as new potential for protection. During the 1980s and 90s, national security threats from cyberattacks began to gain attention.

6.1 First Attacks

In 1988, The Morris Worm was one of the first widespread attacks on national security, causing significant disruptions and showing the vulnerabilities in networked systems. "When the first solution worked, nearly 6000 – around 10% of the total number of computers in the world – were infected." (Kraken, 2019). This caused a lot of disruption, slowing down numerous systems and crashing affected systems. Many institutions had to disconnect from the internet to get rid of the worm, which caused a lot of downtime.

6.2 State Sponsored Attacks

Cyberattacks sponsored by states increased in frequency in the early 2000s. A couple of noteworthy instances are the Moonlight Maze attacks, which broke into U.S. government networks, and the Titan Rain attack, which was attributed to China and targeted defense companies in the United States. Many foreign governments have faced cyberattacks that have been extremely harmful to the economy and perceptions of government. An example of this was seen in 2007 when Estonia faced a massive cyberattack targeting its government, financial, and media institutions, attributed to Russian actors. This attack was a wake-up call since after this event, "Estonians become experts in cyber defence today" (McGuinness, 2017). The potential for cyberwarfare to interfere with national infrastructure was highlighted by this attack, showing that even national governments were prone to cyberattacks.

6.3 AI powered cyber attacks

In the 2010s, AI started to have two roles in cybersecurity. On one hand, advanced analytics, machine learning, and automated responses provided by AI-driven security solutions enhanced the capacity to identify and address potential threats. However, AI also made it possible for more advanced cyberattacks. Artificial intelligence (AI) has the potential to enhance the effectiveness of phishing attacks through the creation of customized messages and the automation of searching for system vulnerabilities. The WannaCry ransomware attack demonstrated the devastating potential of cyberattacks on national security. "The WannaCry ransomware attack occurred on May 12, 2017, and impacted more than 200,000 computers. WannaCry used an unpatched vulnerability to worm across networks all over the world" (What Was the WannaCry Ransomware Attack? | Cloudflare, n.d.). The WannaCry "ransomware worm spread to more than 200,000 computers in over 150 countries. Notable victims included FedEx, Honda, Nissan, and the UK's National Health Service (NHS)," which caused many ambulances to be sent to other hospitals (What Was the WannaCry Ransomware Attack? | Cloudflare, n.d.).

6.4 Uses of AI

The use of automated propagation techniques highlighted the evolving complexity of cyber threats. Cybersecurity threats keep changing as AI is integrated. AI is being used by nation-states more and more to improve their offensive capabilities. Artificial intelligence-driven deepfake technology is a serious concern since it may produce realistic-looking but fraudulent images and sounds, which might spread false information or destroy public confidence. AI-powered cyber espionage tools are also growing, providing attackers with increased capacity to break into networks, obtain data, and damage operations.

6.5 Government Policies

Governments are spending more money on AI to strengthen their cybersecurity defenses. National security policies are increasingly reliant on AI-driven threat intelligence platforms, anomaly detection systems, and automated incident response tools. The relationship between cybersecurity and national security will get more intricate as AI technology develops. Governments will have to create strong plans to combat cyberattacks that are aided by AI, as well as use AI to strengthen their own defenses. To sustain national security in the face of growing cyber threats, international cooperation, sophisticated threat detection systems, and ongoing innovation in cybersecurity techniques will be essential. In conclusion, from relatively basic exploits to highly sophisticated, state-sponsored campaigns, cybersecurity attacks on national security have changed throughout time. The incorporation of artificial intelligence (AI) into cyber operations, both offensive and defensive, represents a substantial change in the environment that calls for constant adaptation and attention to safeguard vital infrastructure and national interests.

7 Cyberattacks in the Healthcare Industry

Healthcare cybersecurity is a major area of concern, particularly as the sector gets more digitalized. The use of artificial intelligence (AI) in healthcare has resulted in important improvements as well as new difficulties with regard to the security of private medical data.

7.1 Digitalized Health Care

From the 1990s to the 2000s, the Electronic Health Records (EHRs) marked the beginning of the digitalization of medical records. Although this shift increased effectiveness and patient care, it also created new security holes. Because early cybersecurity safeguards frequently lacked proper security, cybercriminals found healthcare institutions to be appealing targets. "While EHR use has increased and clinicians are being prepared to practice in an EHR-mediated world, technical issues have been overshadowed by procedural, professional, social, political, and especially ethical issues as well as the need for compliance with standards and information security" (Evans, 2016). In 2015, nearly 80 million people's personal information was compromised in the Anthem Inc. data breach, underscoring the serious effects of cyberattacks on the healthcare industry. Names, addresses, Social Security numbers, dates of birth, medical IDs, insurance membership numbers, income information, and job details were among the compromised data. In 2017, Global healthcare systems were impacted by the WannaCry ransomware assault, with the National Health Service (NHS) in the UK being the most affected. The incident affected hospital operations and brought attention to how important it is for the industry to have strong cybersecurity safeguards. Fortunately, the ability to identify and respond to cyber threats has greatly improved thanks to AI-driven technologies.

Figure 5 This image shows how healthcare has become very digitalized and imbued

7.2 AI Capabilities in Health Care

Large volumes of data may be analyzed by machine learning algorithms, which can then instantly spot odd trends and possible dangers. The time it takes to mitigate assaults can be decreased by these systems' ability to react to some threats automatically. AI can predict dangers and vulnerabilities before they occur. AI systems can predict where and how future attacks might occur by analyzing historical data and identifying trends. This ability enables healthcare organizations to proactively strengthen their defenses. Processes for automating incident response can be aided by AI. AI technologies, for instance, can reduce the effect of an attack on healthcare operations by separating hacked systems, blocking harmful traffic, and restoring data from backups. By monitoring access controls and making sure that only authorized workers have access to sensitive information, AI can help protect patient data. Security personnel can be promptly notified by AI algorithms that identify attempts at illegal entry. However, data privacy is an issue when using AI in healthcare.

7.3 Staying protected from threats

Maintaining trust and adhering to laws like the Health Insurance Portability and Accountability Act (HIPAA) requires making sure patient data is anonymous and maintained securely. As AI technology develops, so do cybercriminals' strategies. Deepfakes and other sophisticated phishing tactics are examples of AI-powered attacks that provide new difficulties for healthcare cybersecurity. Advanced AI-driven cybersecurity solutions can require a lot of resources to implement. Healthcare businesses, particularly those with smaller operations, may encounter difficulties with resources, knowledge, and infrastructure. To keep ahead of new risks, healthcare institutions might gain from working together and exchanging threat intelligence. Collaborative cybersecurity resilience can be improved by industry-wide initiatives and public-private collaborations. In order to combat evolving cyber risks, the healthcare industry needs to consistently innovate and incorporate new technologies. This entails improving security measures by utilizing developments in blockchain, artificial intelligence, and other cutting-edge technology.

In summary, there is a great deal of promise for enhancing the security of private medical data and guaranteeing the availability of healthcare services through the incorporation of AI into cybersecurity in the healthcare industry. To counter the constantly changing world of cyber dangers, nevertheless, cooperation, investment, and constant monitoring are also necessary.

8 Solutions to Ai driven Cyberattacks

As we cover all of the different ways that cybercriminals are able to bypass defenses and mechanisms, it is crucial to look at how our protection and cyberdefenses can change and overcome these issues. Cybersecurity analysts and engineers are constantly being forced to adapt and change their methods in order to keep their methods and techniques effective and working. One of the most recent and promising solutions and innovations in the cybersecurity field is the usage of AI in order to strengthen and improve current system architectures.

8.1 AI Automated Analyzation

One of AI's greatest strengths lies in its ability to analyze large amounts of data and behaviors much faster than any human can. This allows for AI to be utilized in threat detection and responses with its automated detection and incident response capabilities. Another form of this is when AI tracks specific user behaviors to determine if it is fraudulent or something that needs to be flagged. Another important task of a cybersecurity analyst is to perform risk and vulnerability assessments. Ai is able to constantly automate checks for different issues or weak points within a system, allowing it to be fixed and strengthen the overall system. Another potential use of AI is in penetration testing in which developed AI tools can target one's own technology in order to provide a better understanding of what is needed to be improved before a cybercriminal can maliciously exploit it. Machine learning allows these new AI-integrated software to constantly learn and improve itself from past experiences, thus allowing the applications to gain threat intelligence and become more accurate.

8.2 Reducing Human Error

Often times these cybersecurity systems are put in place to protect important servers and data structures that are vital to be kept well, allowing many processes and services to keep running. As humans work and update these tools and updates there is a great chance of error occurring from things like misspellings, and syntax errors. These errors can cause catastrophic issues if implemented, potentially leaving servers down and allowing CyberCriminals a point from which to enter. AI reduces the chance of these errors recurring from manually entered data sets and is able to automatically detect any of these anomalies in a data set that humans may miss.

8.3 Defending DDoS attacks

A major issue that many servers face is the threat of DDoS attacks that are capable of overwhelming a website or network until it inevitably crashes. This can be easily protected against as "AI is a useful tool for recognizing and blocking bots based on behavior or IP addresses that are inconsistent with human behavior"(Dashlane, 2023). This allows for there to be an automatic reading of any incoming packets or data to ensure that no malicious behavior transpires without manual supervision.

8.4 Improving IDs Systems

While AI is commonly used to carry out actions on its own, another feature is the way that it can read through incident-related data and display it for a security team. This then assists the team by allowing them to take action in containing the threat much quicker than normally. An example of this is the use of an Intrusion Detection System(IDS). These systems are put into place to monitor network traffic and devices for malicious or suspicious activity. The one major downfall of this device is that they commonly ping false alarms as they rely on only known behaviors, which may not indicate a threat. To improve upon this, cybersecurity analysts can deploy AI methods such as Artificial Neural Networks(ANN) into their IDS. This improves the detection rate as "However ANN would be capable of detecting when a connection is legitimate and when it should trigger a security alert due to the connection patterns"(Calderon, 2019). Even though cybercriminals attempt to use unpredictable and unrecognizable patterns when avoiding detection, this Machine learning-centered approach would be able to still detect it as a threat to the server. This is further enhanced as "AI-based IDS can learn and adapt to new threats and the changing network behavior over time"(MARKEVYCH et al., 2023). This then enables the AI-driven IDS system to adapt and detect new attacks that were never before seen.

8.5 Real World Data

A real-world example of these AI-driven detection systems can be seen when "The Siemens Cyber Defense Center (CDC) used AWS (Amazon Web Services) to build an AI-enabled, high-speed, fully automated, and highly scalable platform to evaluate 60,000 potentially critical threats per second" (LAZIC, 2019). This allows them to scan and monitor threats at a rate far greater than any human while also staying accurate, thus allowing the system to stay at optimal performance and not require as many people on the team. More research shows that "With AI, the overall time taken to detect threats and breaches is reduced by up to 12%"(LAZIC, 2019). This ensures that Cybersecurity analysts can respond to threats

as quickly as possible, potentially saving a substantial amount of money and infrastructure (Mohammed, 2024). This revolutionizing form of cyberdefenses is also growing and being innovated upon at a rapid pace to become smarter and more effective as shown by "A recent research report estimated the global market for AI-based cybersecurity products was about $15 billion in 2021 and will surge to roughly $135 billion by 2030.3"(Morgan Stanley, 2023).

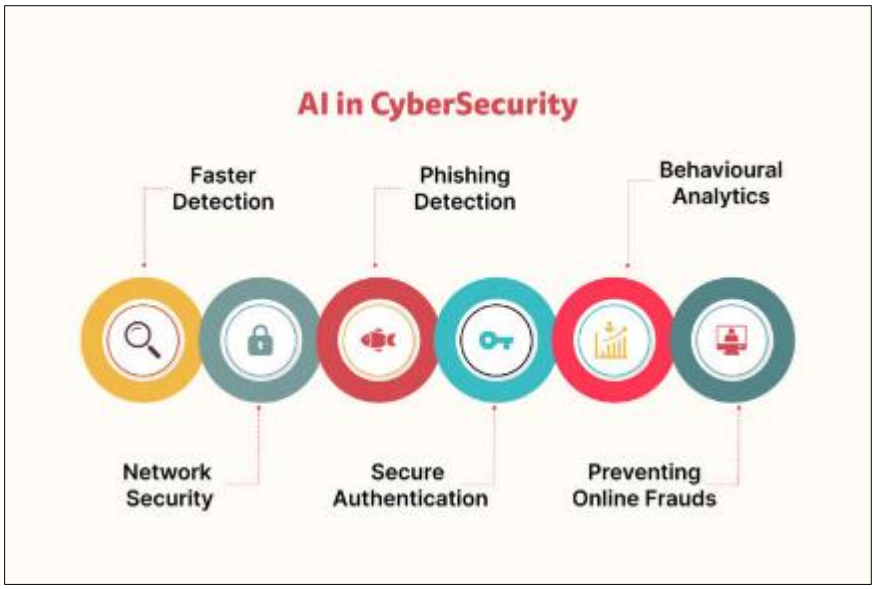

Figure 6 The various ways in which Ai can assist in and strengthen cybersecurity architectures

9 Conclusion

It is obvious that to keep up with these threats, our cybersecurity defenses must constantly change as we have examined the several methods by which cybercriminals take advantage of weaknesses. AI in cybersecurity offers a promising way to improve our defenses. With AI's proficiency in automated analysis, predictive analytics, and adaptive defenses, cyberattacks may be identified, stopped, and dealt with more skillfully. We can create more robust systems that can withstand the constantly evolving threat landscape by adopting these AI-driven solutions.

References

[1] Mohammed, Z. A., Mohammed, M., Mohammed, S., & Syed, M. (2014). Artificial Intelligence: Cybersecurity Threats in Pharmaceutical IT Systems.

[2] Dash, B., & Sharma, P. (2023). Are ChatGPT and deepfake algorithms endangering the cybersecurity industry? A review. International Journal of Engineering and Applied Sciences, 10(1), 21-39.

[3] Knight, P. (2000). ILOVEYOU: Viruses, paranoia, and the environment of risk. The Sociological Review, 48(2_suppl), 17-30.

[4] Stratejm Inc. (2023, January 26). Ai and cybersecurity: Is chatgpt a threat?. Stratejm. https://stratejm.com/ai-and-cybersecurity/

[5] Joseph, L. (2024, May 16). A quarter of UK business are not using AI to bolster cybersecurity - IT security guru. IT Security Guru - The Site for our Community. https://www.itsecurityguru.org/2024/04/10/a-quarter-of-uk-business-are-not-using-ai-to-bolster-cybersecurity/

[6] Hong, S. (1970, January 1). SPT V7N3 - man and machine in the 1960s. Virginia Tech Scholarly Communication University Libraries. https://scholar.lib.vt.edu/ejournals/SPT/v7n3/hong.html#:~:text=In%20the%20mid%2D1960s%2C%20computers,the%20post%20office%20and%20supermarkets.

[7] Gcu. (2019, September 16). A look at the history of cybersecurity. GCU. https://www.gcu.edu/blog/engineering-technology/look-history-cybersecurity.

[8] Bekshentayeva, K. (2015). Detection of denial of service attacks using Echo State ... https://summit.sfu.ca/_flysystem/fedora/2022-11/etd21574.pdf

[9] Knight, P. (2000). ILOVEYOU: Viruses, Paranoia, and the Environment of Risk. The Sociological Review, 48(2_suppl), 17-30. https://doi.org/10.1111/j.1467-954X.2000.tb03518.x

[10] McGuinness, D. (2017, April 27). How a cyber attack transformed Estonia. BBC News. https://www.bbc.com/news/39655415.

[11] Evans R. S. (2016). Electronic Health Records: Then, Now, and in the Future. Yearbook of medical informatics, Suppl 1(Suppl 1), S48–S61. https://doi.org/10.15265/IYS-2016-s006.

[12] Stanham, L. (2024, May 31). Most common AI-powered cyberattacks - crowdstrike. crowdstrike.com. https://www.crowdstrike.com/cybersecurity-101/cyberattacks/ai-powered-cyberattacks/

[13] Novaes Neto, N., Madnick, S., Moraes G. de Paula, A., & Malara Borges, N. (2020, March 17). A case study of the Capital One Data Breach. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3542567

[14] Detecting and characterizing web bot traffic in a large E- ... (n.d.). https://www.eecis.udel.edu/~hnw/paper/esorics18.pdf

[15] Warren, P., Kaivanto, K., & Prince, D. (2018). Could a cyber attack cause a systemic impact in the financial sector? Bank of England Quarterly Bulletin, 1–10.

[16] Stanham, L. (2024, May 31). Most common AI-powered cyberattacks - crowdstrike. crowdstrike.com. https://www.crowdstrike.com/cybersecurity-101/cyberattacks/ai-powered-cyberattacks/

[17] White, K. (2024, March 6). Real-Life examples of how AI was used to breach businesses. New. https://oxen.tech/blog/real-life-examples-of-how-ai-was-used-to-breach-businesses-omaha-ne/

[18] Calderon, R. (n.d.). The benefits of artificial intelligence in Cybersecurity. La Salle University Digital Commons. https://digitalcommons.lasalle.edu/ecf_capstones/36/

[19] Mohammed, S. (2024). AI-Driven Drug Discovery: Innovations and Challenges.

[20] Ai and cybersecurity: A new era. Morgan Stanley. (2023). https://www.morganstanley.com/articles/ai-cybersecurity-new-era.