e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 5, Issue 12, December 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.54

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly, Peer Reviewed & Referred Journal|

| Volume 5, Issue 12, December 2022 |

| DOI:10.15680/IJMRSET.2022.0512027 |

Challenges, Threats, and Mitigation in the Field of Artificial Intelligence for Cybersecurity

Vikesh Kumar Singh, Dr. Istiyaque Ahmad

Scholar, Department of Computer Science, Sunrise University, Alwar, Rajasthan, India

Research Supervisor, Assistant Professor, Department of Computer Science, Sunrise University, Alwar, Rajasthan, India

ABSTRACT: Now that we live in the digital age, technology has made it possible to automate almost every aspect of daily life. But technology still hasn't given individuals enough protections and capabilities. Concerns about the safety of all these internet-connected gadgets are growing exponentially as the number of devices linked to the internet continues to rise. In recent years, reports of data breaches, identity theft, fraudulent transactions, compromised passwords, and compromised systems have become commonplace in the headlines. The growing threat of cyberattacks was caught off guard by the latest developments in artificial intelligence. Almost every branch of engineering and research is finding some use for AI. Artificial intelligence (AI) not only automates a certain activity, but it also significantly increases efficiency. It follows that hackers would find such a delicious buffet to be quite enticing. As a result, traditional cyberattacks and threats have evolved into "intelligent" ones. Conventional and intelligent defences against cyber-attacks are covered in this article, along with cybersecurity and cyber dangers. In addition, before we wrap up, let's talk about what the future holds for AI in cybersecurity.

KEYWORDS: Cybersecurity, Cyber-attacks, DDoS, Man-in-the Middle, Intrusion Detection, Artificial Intelligence.

I. INTRODUCTION

Almost every organisation, household, and business these days makes use of some kind of internet connection. The sheer number of electronic gadgets and applications that the average person uses on a daily basis might be overwhelming. Even with the best of intentions, many of us are unable to limit our use of electronic devices. Some people may have an unhealthy obsession with the internet and never be able to cut down, while others may not use it nearly enough to stay up with the technological advances. Instead of communicating with others, some people could spend hours on end staring at their phones or laptops. We can't help but utilise the internet for everything since it is such a strong tool. Technology has unquestionably improved our efficiency and production in several ways. The impact on our social life, mental health, and physical health are all factors that must be taken into account, however. Given that

While the widespread availability of Internet-connected gadgets has many positive aspects, the shadow cast by cybercrimes has been ever-present. A lot of people are worried about the possibility of losing their privacy in this highly linked society. Our heightened efficiency and susceptibility to cyber-crime have been accompanied by an exponential growth in our interconnection. We need to be aware of how closely we are tied to the internet. We are both conquerors and pris-oners now, thanks to the internet. The internet has opened up hitherto unimaginable channels of communication. On the other hand, this has also made everything more susceptible to cyberattacks.

When criminals conduct fraud, steal data, or inflict harm using digital media, they are committing cyber-crime. In essence, any unlawful activity that begins with the use of computers is considered cyber-crime. This includes a wide range of crimes, including but not limited to hacking, phishing, malware distribution, online stalking, and identity theft. Among today's most profitable crimes, cybercrime has emerged as a major player. By stealing information, altering data, and breaching vital infrastructure, hackers earn billions of dollars annually. Cybercrime, like other forms of criminality, has changed and will change significantly throughout the years.

Businesses, governments, and people would all be better protected if cybersecurity is handled holistically, according to a research from "The World Economic Forum" [2]. Additionally, it claims that there is a huge disparity between our present level of preparedness and what is needed to secure cyberspace. We must immediately begin to bridge this gap

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly, Peer Reviewed & Referred Journal|

| Volume 5, Issue 12, December 2022 |

| DOI:10.15680/IJMRSET.2022.0512027 |

before it is too late. Protecting infrastructure from external threats like viruses, malware, or hacking attempts has made cyber security an essential component of every modern system. But external threats account for a small fraction of security breaches and cybercrimes; the vast majority occur as a result of human mistake. Everyone must do their part to prevent cybercrime and ensure the safety of our nation's essential infrastructure.

Data security has just recently come to light, despite the fact that viruses and malware have been an issue since the dawn of computers. The current uptick in hacking is opening up additional opportunities for these "cybercriminals" on the internet. Having stated that, this exposure gives rise to several dangers. Hackers are a real threat since they may disrupt websites, steal data from our systems, and perpetrate fraudulent transactions, among other things. Cybercrime is a new subfield of traditional criminal investigations.

The exponential growth of cybercrime is a direct result of the massive expansion of internet access to over 5 billion people worldwide, or nearly 63% of the total population. Cybercrime is projected to cause around 6 trillion USD in damages by 2021 [1], making it the third-largest economy in the world when assessed independently. From a mere $3 trillion in 2015, Cybersecurity Ventures estimates that the entire cost of cybercrime will rise to $10.5 trillion by 2025 [31]. If recorded history is to be believed, this is the largest ever transfer of wealth. It disincentives new product development and is going to provide more profits than anything we've encountered before. Cybercrime can result in a variety of costs, such as data damage or destruction, restoring or deleting compromised data, financial loss, decreased productivity, theft of intellectual property, embezzlement (the practice of taking assets for the benefit of the person credited with the crime), and damage to reputation. The creation of a more secure system from the beginning, the prevention of cyber-crime, and the reduction of its damage when it does occur are now interdisciplinary endeavours.

It is critical that we take precautions to avoid becoming victims of cybercrime, which is on the rise. One of the most essential things we can do is be mindful of where we are and how we use our personal information online. There are numerous more methods as well. Most of the dangers that are coming into the internet could be avoided if we were just cautious about what we were doing. When it comes to protecting oneself against cybercrime, there are several options available. Installing firewall, antivirus, and internet security software on the device is one approach to protect it. Another way is by using strong passwords and changing them often. Lastly, keeping the operating system updated with the latest patches and updates. One can also monitor network traffic for vulnerabilities and set up auto-responders to avoid phishing attacks. Furthermore, we should also manage our social media settings and avoid using unsecured Wi-Fi networks in public places. Even just by minimizing how much personal information we share online, we can avoid the risk of being a target of identity theft, cyberstalking, and many more such threats.

In addition to these conventional methods, which are just a stopgap measure at best, the use of AI is an emerging field in the world of cybersecurity. Nowadays, AI is prevalent in almost any and all fields of science, whether from medicine to business or from the military to law enforcement. The use of AI in science is almost ubiquitous. The use of AI in cybercrime is growing at such a rapid rate that it has become one of the significant areas of concern worldwide. AI is a potent tool that is being used to combat many different types of crime. It will be vital for law enforcement agencies worldwide to find new ways to utilize this technology to keep up with the ever-increasing rate of cybercrime. AI is being applied to crime-fighting in a number of different ways. In the case of cybercrime, AI is being used to help identify potential threats, detect patterns that can lead to previous criminal activity, and detect new forms of existing criminal activity. However, AI is also being used as part of a broader research initiative on cybercrime and its perpetrators. Cybercrime data is collected, analyzed, and used to build sophisticated virtual crime scenes that can predict crimes before they happen.

AI can be used to mine data, identify patterns, and predict future events. It can also be used to detect cyber-attacks and prevent them from happening. In the future, AI systems will be able to detect patterns that are not readily apparent to humans, like a possible cyber-attack, by analyzing network traffic and determining if different strings of data are accessed in the same unusual pattern. AI can do many things, and it will continue to evolve and grow to be used in more everyday aspects of our lives.

The entirety of this chapter is divided into a total of four sections. The first section outlines the concept of cybersecurity along with the threats and attack models that hackers commonly use to compromise a computer system. The sec-ond section entails the conventional approaches and methods of mitigating the risks of cyber-attacks. The third section then discusses the AI- based approaches to counter cyber-threats or at least mitigate the risks associated with cyber-attacks. Finally, the fourth and the last section talks about the future scope of AI in cybersecurity.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly, Peer Reviewed & Referred Journal|

| Volume 5, Issue 12, December 2022 |

| DOI:10.15680/IJMRSET.2022.0512027 |

II. CYBERSECURITY

The goal of cybersecurity is to prevent unauthorised access to computer networks and sensitive data. Many methods exist for protecting an organization's data and infrastructure, such as intrusion detection systems, virus protection software, and a steadfast commitment to best practices in information security. Attacks on computer systems that use malicious software or ransomware to steal information, halt digital processes, or corrupt data are examples of cyber security threats. Cybercriminals come in many forms, including hackers, corporate spies, and terrorists [28]. Figure 1 displays the cybersecurity taxonomy. While each kind of hacker may have their own unique motivations for targeting certain organisations, the fact remains that they all represent a serious threat to sensitive information. Cybersecurity has entered a new age with the advent of the Internet. Information security is facing new problems related to both external threats, such criminal hackers and foreign governments, and internal dangers, including data breaches and insider theft. When it comes to important infrastructures, assets, and data, cyber security is a crucial cross-cutting issue. It is of paramount importance to guarantee that defence systems against cyber assaults are thorough and strong, which is why the number of cyber security specialists and the sector overall has seen an impressive upturn.

Securing data and minimising harm from a cyber security event are two aspects of cybersecurity, which encompasses all efforts to protect an institution from cyber attacks. It is possible to divide the study of cybersecurity into five main subfields:
Infrastructure security, application security, network security, cloud security, and IoT security are all important aspects of information technology.

Cybersecurity is a dynamic and intricate area. Knowing the many cyber dangers and how to protect yourself from them is crucial. These days, cyberattacks are almost ubiquitous. Nevertheless, with the right security measures in place, these assaults may be avoided.

Learn about the various cyber-attacks and risks, explore conventional and AI-based defence methods, and find out about the solutions that are now available to mitigate these threats in this article.

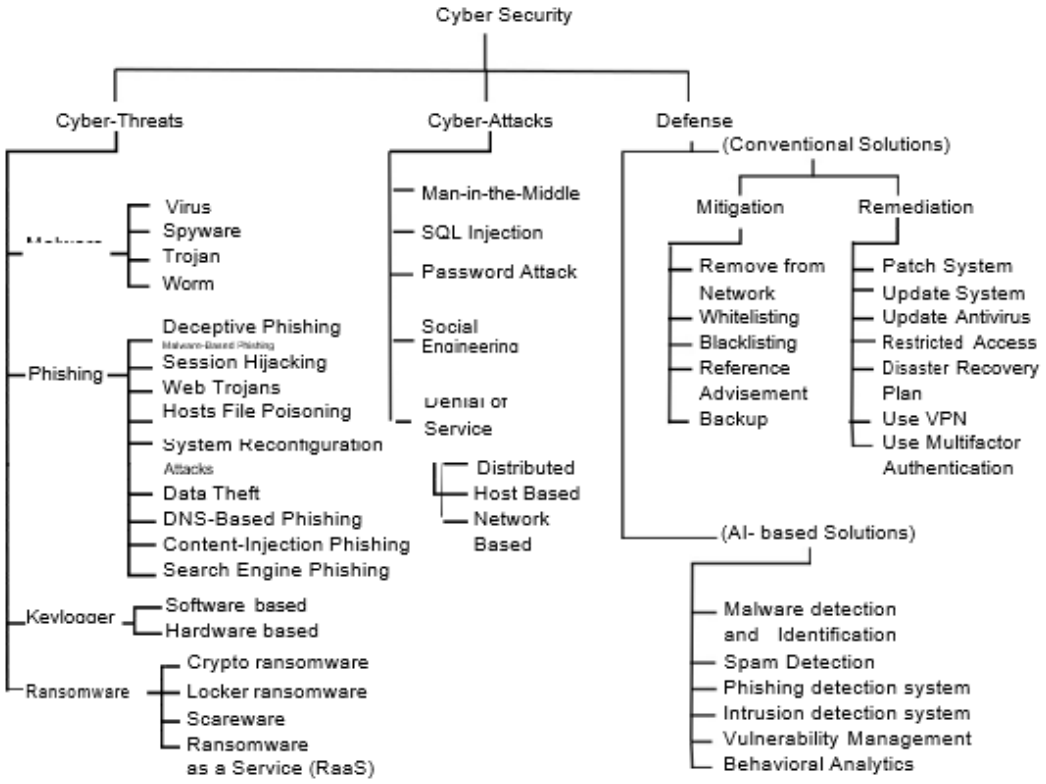

Figure-1: Categorization of cybersecurity

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly, Peer Reviewed & Referred Journal|

| Volume 5, Issue 12, December 2022 |

| DOI:10.15680/IJMRSET.2022.0512027 |

Threat:

Distributed Denial of Service or DDoS : It is a form of cyber-attack where the perpetrator uses multiple systems to flood the target with traffic. The goal is to make it difficult for the target to provide service or access their website. The most common type of DDoS attack is a volumetric attack, which floods the target with an overwhelming amount of data. This can be done by using a botnet, a network of computers that have been infected with malware and are controlled by an attacker without their owner's knowledge. Within the volume attacks category, there are flooding and amplification/reflection attacks. In a flooding attack, traffic is sent in the hopes of exhausting bandwidth, processing capacity, or other network resources. Amplification/reflection attacks seek to force victims to spend money by "overloading" their networks with spam traffic or denying access to certain resources using spam-like messages [36] [27].

There are many tools that can be used to launch a DDoS attack, and the most common is the use of a botnet. The attacker does not need to control the botnet, as they may simply rent it from an online service or purchase it from someone else. Some examples of these services include Blackhole, Stresser, and NitrousDDoS [37].

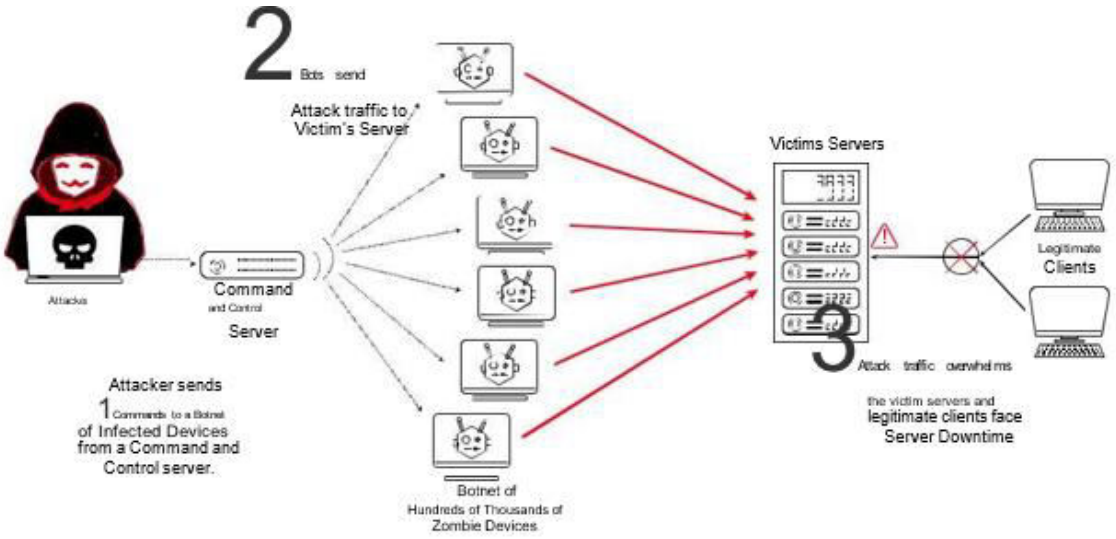

Figure-2: Distributed Denial of Services Attack scenario.

One kind of cyberattack is known as a "Man in the Middle" attack. In this type of assault, the hacker poses as a third party and discreetly transmits or changes the communication between two parties that think they are interacting directly with each other. In addition to reading all communications sent and received between the two systems, the attacker may also insert fake messages. The phrase "man in the middle" originates from an espionage analogy, when an eavesdropper reads both parties' communications while they believe they are speaking directly to each other. There are several techniques to execute a man-in-the-middle attack. The assailant may, for example, sneak up on the two parties and act as a messenger, passing messages back and forth between them. One way to do this is by using a public Wi-Fi hotspot or gaining access to the network of a telecommunications firm and redirecting calls. An other method involves an attacker using a man-in-the-middle (MITM) vulnerability on a remote machine with system admin access to intercept and manipulate client-server communication.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly, Peer Reviewed & Referred Journal|

| Volume 5, Issue 12, December 2022 |

| DOI:10.15680/IJMRSET.2022.0512027 |

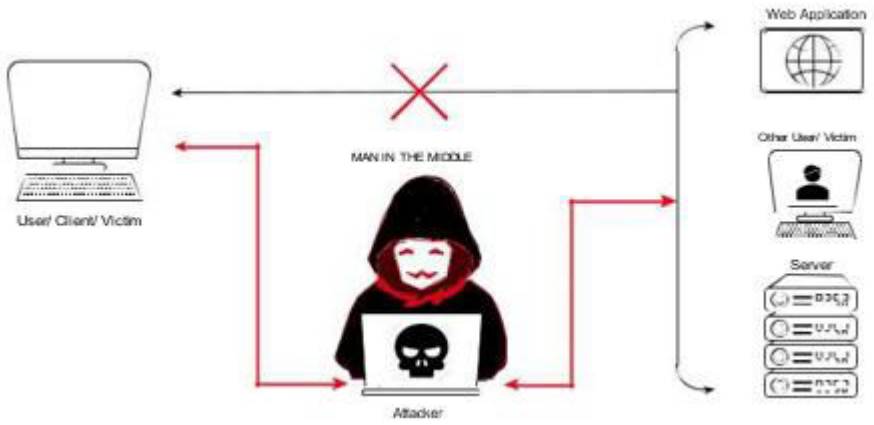

Figure-3: A simple depiction of Man in the Middle Attacks

The term "man-in-the-browser" describes how this kind of attack takes use of security holes in web browsers and other applications. An attacker may use social engineering techniques, such as convincing the user to accept an insecure connection instead of one that uses HTTPS or another secure protocol, or they can take advantage of software vulnerabilities, such Cross-Site Scripting, to launch an attack. It may also describe assaults in which an intruder obtains control of a browser-based machine, then exploits the browser's interface—including the camera, microphone, and recording capabilities—to spy on the user. The perpetrator may then use this data for malicious objectives, such as blackmail.

SQL injection is a kind of cyberattack that takes advantage of a database security hole. This specific kind of code injection attack targets apps that rely on data. Among the many perilous forms of cyberattacks, the SQL injection attack ranks high. It has the potential to compromise databases, alter or remove data, and interrupt service, among other uses. By taking advantage of SQL's (structured query language) inherent dynamic nature, an attacker may bypass input validation and get access to otherwise inaccessible data. An example of SQL injection would be entering a SQL command with incorrect or otherwise incorrect data. Instead of "insert into users values (username, password)," you may send "select password from users" to capture the password after placing it into an account table. As a consequence, the database processes the query and returns the username; an attacker may then use this list to guess passwords for database users. It is also possible to alter table data without authorisation via SQL injection. This might cause the table in question, or any tables that use it, to become unavailable or lose its confidentially.

An attack involving the guessing or outright theft of passwords, often by hacking into a computer system or network, is known as a password attack. An attacker might get access to the victim's account by intercepting their password and using a man-in-the-middle attack. Although sophisticated cracking tools and techniques make short work of passwords, hackers may nevertheless manage to crack them. Brute force, dictionary, and keylogging are the three main categories of password assaults. Being aware of these helps lessen the likelihood of an assault. By repeatedly trying different password guesses, an attacker may get access to a system via a brute force assault. In a dictionary attack, the hacker tries a variety of word combinations in the hopes of eventually finding the correct password. Password recovery attacks may benefit from keylogging, which involves recording keystrokes in order to retrieve sensitive information. Use of two-factor authentication or the practice of avoiding links in emails from unknown senders are two ways to protect yourself against this kind of attack.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly, Peer Reviewed & Referred Journal|

| Volume 5, Issue 12, December 2022 |

| DOI:10.15680/IJMRSET.2022.0512027 |

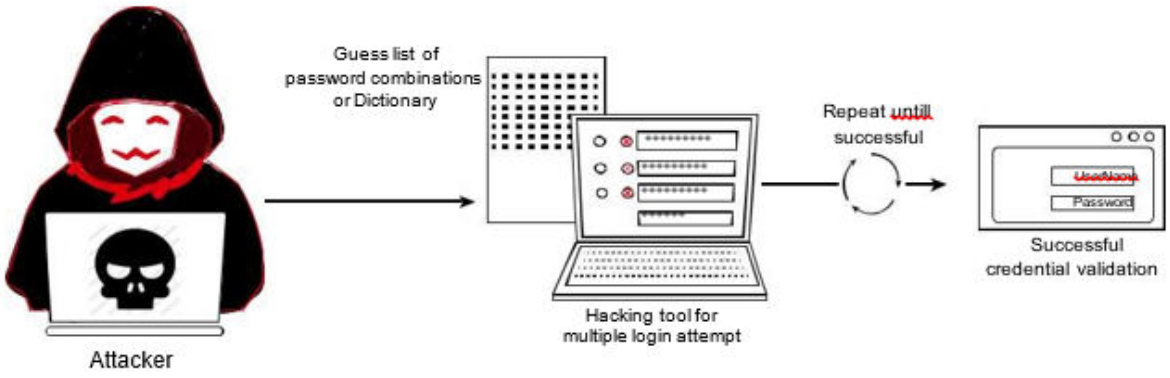

Figure 5. Depiction of generalised principle of a Password Attack

Attacks on the "Internet of Things" (IoT): The "Internet of Things" (IoT) is a network that allows commonplace objects to exchange data and coordinate their movements via the use of embedded electronics, software, sensors, and connections. Among the many possible Internet of Things networks, the most common ones are enterprise intranets and the Internet itself. The Internet of Things is still relatively unknown to cybercriminals. Internet of Things devices are easy targets for fraudsters due to inadequate security measures. Because of this, hackers attack them often. Due to the exponential growth in the number of connected devices, safeguarding them from malicious hackers and cybercriminals has become critical. A Trusted Platform Module (TPM), security standards, and an Internet of Things (IoT) security architecture are the three cornerstones of an IoT security framework [14].

"Cyber Threats to the Internet of Things: Emerging Risks and Tactical Strategies" is the title of a research by Cisco Systems. Among the many goals of these cybercriminals is to steal data, disrupt services, or get access to sensitive personal information stored on the ever-growing number of devices linked to the Internet.

Income from buyers. The paper states that organisations should consider cybersecurity concerns since the Internet of Things will alter the perspectives of both enterprises and consumers. Companies should evaluate the safety of their present network offerings in front of these new dangers.

It would seem that home-based enterprises will remain popular, since the recent pandemic gave a significant boost to the work-from-home culture. This tendency is making residential areas more appealing targets. Everyone agrees that most businesses have good cyber defences, but that's only when you consider their internal networks. When employees use their own devices to access company servers from home, the servers are more likely to be attacked. Microsoft reported a 35% increase in the frequency of these attacks between the second and first half of 2019 and 2020. Due to their ubiquity, home-based office equipment are becoming an increasingly tempting target for hackers. If a hacker caused chaos within the company by breaking into one or more nearby homes, it's quite probable that more houses may be next. To illustrate the point, a de-authentication attack on an unsecured wireless network may potentially provide a hashed password. Furthermore, this leaves the door open for the password to be cracked offline and used maliciously.

Threats

Software that is designed to steal information, harm or destroy computer systems, or gain access to private computer networks is known as malware. Malware often masquerades as 'ad-ware,' or seemingly legal software, but when run, it really performs some secret task.

Different types of malware may be categorised according to how they infect:

- Viruses: These are computer programs that may infect other files and create copies of themselves. They often propagate via contaminated data copied onto a CD or DVD, infected files downloaded from the internet, or email attachments.
- Worms: These are programs that can replicate themselves and spread over the internet by using a computer's network connections. They may propagate on their own, without the help of humans.
- Trojan horses: These harmful programs masquerade as something else, usually a valuable commodity, and carry out destructive operations.

According to Cisco, malware has the ability to block critical network access, install other malicious software, and

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly, Peer Reviewed & Referred Journal|

| Volume 5, Issue 12, December 2022 |

| DOI:10.15680/IJMRSET.2022.0512027 |

transfer data from hard drives. While Cisco Ta-los cybersecurity experts did find a kind of malware dubbed Responder being used to commit DDoS assaults, the firm is choosing not to name any of the organisations implicated in the incident. The hacker Peter Severa developed Responder, which the corporation says is available for download on dark web sites.

One kind of cyber-threat that is on the rise is phishing. A kind of social engineering, it involves using deception to get others to provide sensitive information. When a hacker sends an email with the intention of tricking a target into opening an attachment or clicking on a link, they are engaging in the most prevalent kind of phishing. A phishing website may seem identical to the actual one and request login information if you click on the link. The file might include malicious software that encrypts files or steals personal information. In order to trick their targets into believing they are dealing with a trustworthy entity, phishers often craft emails that seem to originate from well-known brands.

In order to trick their targets, phishers are becoming craftier and craftier, adopting tactics including DNS-based phishing, host file poisoning, web trojans, session hijacking, and malware-based phishing [35]. As part of this scam, cybercriminals pose as legitimate businesses in an email in an attempt to trick victims into divulging sensitive information. The objective is to get access to the user's accounts or steal their identity by making them believe they are engaging with a real firm.

Phishing that uses deception is the most prevalent kind. Phishing in this context refers to the practice of using fraudulent websites to acquire sensitive information (email addresses, passwords, credit card numbers, etc.). There is no proof that the majority of individuals are aware of or trust this kind of phishing, and there is also no proof that these approaches work. One benefit of phishing assaults is that they are not limited by geographical limits. This is due to the fact that anybody, at any time, may access a computer. The fact that the victim gets nothing in exchange for divulging their personal details makes phishing assaults a "low-risk" threat, which is another plus. On the other hand, cyberstalking occurs when an individual uses social engineering techniques, such as impersonating another person or creating a false account with a similar name, to send a hostile message.

Another kind of cybercrime is cryptojacking, which occurs when malicious software takes over a computer and uses its computing power to mine bitcoin. Malware infiltrates applications such as web browsers, scripts, and advertisements, and then stealthily uses the infected device's processing power to mine cryptocurrency. The cybersecurity firm McAfee first used the word "cryptojacking" in 2017. Cryptojacking is a combination of the words "cryptocurrency" and "hijacking." One way to do cryptojacking is to install malware on the victim's device. This will allow the malware to mine cryptocurrency using the victim's device's resources.

- Sites that secretly mine bitcoin on users' devices using scripts without their awareness or permission.
- A device infected with mining software.

There has been a surge in coin-mining malware due to the rising value of cryptocurrencies. In order to mine cryptocurrency, many of these malware infect machines and take over their resources. Additionally, programs may be found on some websites that mine bitcoin on gadgets used by their guests without their permission or knowledge. Coinhive is a popular example; it uses the devices of website users to mine bitcoin. Affected devices may experience reduced performance and battery life as a consequence of this. It's also possible to steal cryptocurrency via coin-mining malware. Hackers have developed mining software that steals Monero and other cryptocurrencies by covertly stealing the processing power of machines. Installing the right security on your devices may easily avoid most infections, including harmful coin-mining software, even if the risk is great.

Destructive virus known as ransomware encrypts user data and then demands payment in order to unlock it. This kind of cyberattack has grown in popularity over the last several years. Some malware has been given this name as well; it refers to "ransomware-as-a-service," a subset of ransomware that circulates in underground "crypto marketplaces" on the dark web.

Any private citizen or group of individuals not associated with any official authority may launch a ransomware assault. It is difficult to track down the perpetrators since Bitcoin is the currency demanded by the attackers. An unknown ransomware malware known as Petya affected systems all across the globe in May 2017, marking the first observation of the assault. Malicious software known as ransomware attacks susceptible equipment (such as computers or servers) and encrypts them, making them unusable until the victim pays a ransom to decrypt them. By encrypting all data on the machine and taking advantage of a Windows OS vulnerability, Petya employs malware that was created by the NSA to

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly, Peer Reviewed & Referred Journal|

| Volume 5, Issue 12, December 2022 |

| DOI:10.15680/IJMRSET.2022.0512027 |

propagate. After then, the program will make a screenshot including a ransom note requesting $300 in bitcoin in order to decrypt the user's data. But Petya is undetectable, unlike other ransomware systems. Among the consequences of a ransomware attack are:

The disruption of data and processes caused by ransomware attacks may have a chilling effect on businesses, as it sows seeds of fear and uncertainty.The ransomware attack's expenses are hard to put a price on, but they're probably rather high. -Encrypting data makes a business more susceptible to cyberattacks in the future.

Keyloggers are among the most prevalent forms of malware that secretly record sensitive information, including login credentials for online accounts, financial details, and email accounts. An intruder might use specialised hardware or software called a keylogger to secretly record the user's keystrokes if a computer system has a keyboard connected. Passwords, personal details, and other sensitive information are often the targets of these types of attacks. Inserting a keystroke logger between the keyboard and the computer's CPU allows it to record keystrokes as they are deciphered by the BIOS or operating system. The loggers may sometimes be positioned situated on the motherboard. One notable instance of keylogging being used in espionage is the August 2001 FBI investigation into John Walker Lindh, often known as the so-called American Taliban. To do this, a keylogger program is installed on the compromised computer and a screenshot of the victim's active keyboard is captured. The keylogger software keeps track of the keys pressed, together with information about where they are on the keyboard and the applications that utilised them. It is possible to set the keylogger software to launch automatically whenever the machine starts. In this way, the program may record the user's keystrokes for future reference and to build a profile of their computing habits. To facilitate further investigation, the log files are preserved on the hard drive and may be retrieved at a later time. Any computer with a regular web browser may install the free program, and it is available in a broad range of languages. It records keystrokes in two formats: "scores" produced by the OS and "patterns" produced by the user's individual typing habits. The log files are not kept in RAM but on the hard disc. The encryption key used to secure the pattern data is computer-specific and can only be decrypted with the user's password. So, unless you know the password or can get into the system, it's not possible to extract the patterns from a hard drive. However, if someone were to gain access to your computer, they could read this data in its exact form.

1.2 Employing AI in Cyber Attacks

The internet's ability to function due in large part to its decentralised structure. It would be impossible for a single body to manage or shut down the internet since it is not controlled by just one. This one-of-a-kind feature of the internet helped it succeed and paved the way for innovations like artificial intelligence. But as AI grows in popularity, the web has the potential to transform into something quite new. For example, the ability to influence public opinion (by spreading false information that causes herd mentality) or even start wars might be achieved via the management of internet traffic by AI. The Singularity was one of the most well-known causes that paved the way for artificial intelligence. The theoretical idea of singularity describes a future in which technology progress reaches a breaking point and causes technological development to spiral out of control. A "post-human" age when computers' intellect exceeds that of humans is the end outcome. In spite of the fact that no one has yet figured out how to halt an AI with virus-creating capabilities, the concept has recently gained a lot of traction.

Malicious software that is able to elude antivirus programs may be developed using AI. False profiles may be created and false information can be distributed on social media using this. The intelligence and military sectors rely on AI to detect and label certain items in images. When AI can make judgements on its own, such the optimal number of casualties to shoot based on an estimated crime rate, there is a high risk that it will be abused. More than 60% of transactions are executed by AI, while a 2019 research found that more than 92% of Forex trading was done by AI rather than humans [21]. AI is also being used to forecast stock market catastrophes. There will likely be a dramatic increase in the use of algorithms to execute above $10M in the next four years.

III. CONVENTIONAL SOLUTIONS

Network security, which includes intrusion detection systems, antivirus software, encryption technologies, and firewalls, is the most typical line of defence against cyber attacks. Network security is helpful, but it won't fix everything. Since there will always be security holes that malicious actors might exploit, experts believe that no system can be considered completely safe. As part of a comprehensive cybersecurity plan, network security is an important consideration. Consequently, cloud security is the process of preventing unauthorised access to data kept in cloud computing environments like Microsoft Azure or Amazon Web Services (AWS). One common practice is to encrypt

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly, Peer Reviewed & Referred Journal|

| Volume 5, Issue 12, December 2022 |

| DOI:10.15680/IJMRSET.2022.0512027 |

data before keeping it on the cloud, especially when dealing with sensitive client information. To do this, one may use the public key infrastructure or a similar system.

To lessen the blow of security breaches, organisations use cybersecurity strategies that include policies, processes, and methods. It consists of measures to lessen the impact of dangers including hacking, data breaches, and harmful programs. Risk assessment, one part of a cybersecurity plan, looks at the possibilities of an event happening and how likely it is that it would have an impact. Various forms of danger and weak spots in an organization's defences are often considered in a risk assessment. Whether a company's website is hackable or whether password security is inadequate are two examples of factors that might be considered in an evaluation. It is possible to lessen the occurrence or severity of cybersecurity incidents by developing mitigation strategies once risks have been evaluated. Risks of cybersecurity incidents may be lessened by the use of mitigation strategies. Patching, encryption, and security controls are the most popular forms of mitigation.

Organisations that want to exert more control over many facets of their digital security might benefit from the Zero trust policy, one of several such policies. By analysing resources and past user history, it guarantees that firms can regulate sensitive information access. Employee privacy and the mitigation of data breach risks are both enabled by the zero trust policy. Applications and data management, email communication, company-owned or -provided mobile applications and apps, suppliers of cloud computing, infrastructure, or storage services, and company-used terminals are all subject to the zero-trust policy. All parties involved, including businesses, workers, and people' right to privacy, stand to gain from the zero-trust approach. In doing so, it facilitates the development of secure digital identities and the opening of doors for access in times of necessity. An information security strategy known as a zero-trust policy allows end users to access any other user's computer or program without assuming any trust. As a method of information security, the zero trust policy (also called the no trust policy) allows end users to access any other user's computer or application without establishing a trust connection. As a result, creating a paradigm known as "penetration of trusted computing" that mandates certain conditions for all users and devices to satisfy before to accessing network resources. The notion of a zero-trust approach has been utilised to construct the idea of an Internet of Things (IoT) that depends on trust-less computing protocols; the word is also used to comprehend cybersecurity. As far as traditional countermeasures against cyber threats are concerned, the following tactics have been implemented:

The use of firewall and antivirus software:
In order to protect a computer system from viruses and other harmful software, a firewall is a piece of hardware or software that divides the system from the internet. Organisations have more control over incoming and outgoing traffic via firewalls, which operate as a barrier between the network and the outside world. The same holds true for antivirus software; it scans for and eliminates dangerous threats the moment they launch. It is common practice to scan the device and/or network for malware and eliminate it as part of this procedure. Modern antivirus software, as expected, can do a dual-pronged evaluation of machines. A system scan, on the one hand, examines files for malicious threats and removes them before they can do any further harm to the system. Although it does not remove anything, it does check for malware on the machine. An alternative approach is to conduct a thorough scan. This checks all of the files for viruses and malware and deletes them if found. Although it eliminates the possibility of future damage, the lengthy process of scanning all of the files and erasing them if determined to be harmful is a drawback.

Utilising add-ons for secure web browsing
By preventing phishing and other harmful websites from attempting to steal personal information, a secure browser extension helps users remain safe online. It safeguards against the possibility of viruses and adware simultaneously. As an example, the "HTTPS Everywhere" Firefox add-on compel your browser to use an SSL-encrypted version of a website wherever one is accessible, thereby improving online privacy. By default, "Privacy Badger" prevents third-party tracking of your online activities. With "AdBlock Plus," you can block ads while you surf the web.

Utilising virtual private networks
To safeguard information from hackers, a virtual private network (VPN) is your best bet. It prevents hackers from accessing data by encrypting it and sending it over an encrypted tunnel. There is a kill switch in certain VPNs that, if the connection drops, will immediately cut off all internet activity. Data leakage via peer-to-peer connections may be avoided in this way, which might be useful in certain contexts. A virtual private network's (VPN) ability to encrypt data as it moves between servers is its main selling point. No one, not even ISPs or hackers, will have an easier time obtaining data and surfing histories as a result of this. Additionally, the ultimate destination of the outbound traffic remains undisclosed. In addition, when a user connects to a VPN, their real IP address is "hidden" behind the one assigned by the VPN provider. If you want to surf the web anonymously, this will assist.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly, Peer Reviewed & Referred Journal|

| Volume 5, Issue 12, December 2022 |

| DOI:10.15680/IJMRSET.2022.0512027 |

- Setting up secure and distinct passwords

In order to prevent hackers from easily gaining access to sensitive information, it is crucial to establish strong and unique passwords for all of your online accounts. A strong password is one that is both difficult to remember and simple to use, and it consists of a combination of capital and lowercase characters, numbers, and symbols. So that we don't lose track of which websites and applications need various password types, a password manager may also categorise passwords.

Updates and security channels

Because they keep computers current, security updates are crucial. Even though it's annoying, keeping software updated is essential for the device's and the network's health. Attackers will attempt to take advantage of both the software that has received a security update and the users who have chosen not to install it.

IV. AI INVOLVEMENT

Cyberattacks using AI is a relatively recent development. The impact on cybercrime going forward is uncertain at this time. Cybersecurity makes use of a wide variety of artificial intelligence and machine learning approaches. Strategies that use AI to detect cyberthreats, keep an eye on suspicious activity, and secure a company's networks are among the most popular. As an example, a malware analyst may teach an AI system to recognise infected computers and harmful files using machine learning methods. Artificial intelligence systems may also monitor human or group behaviour, for as by noticing shifts in social media activity or by examining employee transportation patterns to spot suspicious activities. Data accessibility for cognitive applications that may integrate human supervision and managing data that is accessible across many systems are the primary concerns for organisations when incorporating AI into cybersecurity. Our personal and professional lives have been greatly impacted by artificial intelligence.

4.1 Current Patterns

Accompanying this trend is the growing use of cognitive technologies in cybersecurity. When it comes to cybersecurity, a human-centered, holistic strategy is crucial, and AI-powered cognitive technologies are an integral aspect of that approach. The nature of security threats evolves in tandem with technological advancements, making cyber defence an ever-evolving field. The best cybersecurity experts will be able to protect their organisations from cyberattacks by using effective cognitive technologies and providing their human element with a holistic strategy. A number of long-term trends have also found an audience in the cybersecurity business, such as the growing importance of artificial intelligence and the role that blockchain technology plays in facilitating cyber defence. As a consequence of these changes, the research projects that the size of the IT security workforce will rise. Although it may be difficult to put a price on, cybersecurity is an essential part of every company. Read CyberVance's 2019 Cybersecurity Trends to Keep an Eye On for more on why it's crucial to study emerging patterns in cybersecurity strategy. In particular the best practices for cyber defence and the use of new technologies by organisations.

Cybersecurity experts used to put much of their energy on keeping an eye out for potential dangers and developing strategies to counter them. They have shifted their focus to risk assessment and mitigation in order to ward against potentially harmful exploits. Which brings us to our first and foremost concern: "What is the risk of this type of exploit?"It's clear that cybersecurity professionals are facing a lot of additional adjustments. The emphasis has shifted from threat monitoring to risk mitigation and probability assessment. For those hoping to get into the industry, these innovations have opened up a whole new universe.

Expert Systems and Intelligent agents are a more inclusive way to categorise the AI methods used to identify and mitigate cyberthreats.

A system of experts

Expert Systems are computational tools that can mimic human judgement. The Inference Engine and the Knowledge Base are the two main components of a knowledge-based system. Decisions are based on interpretations or inferences drawn from the data stored in the Knowledge Base, which is connected to the Inference Engine. The data stored in a knowledge base allows a knowledge-based system to draw conclusions and make predictions. They have potential applications in fields as diverse as medicine, finance, and even future prediction. A knowledge-based system is an information processing system that uses stored data in conjunction with a computational engine called an Inference Engine to forecast future values of unknown variables given current values of known variables. Google Search, Alexa, Siri, and the Weather Channel are all instances of such systems. When applied to specific situations, the predictive models developed by knowledge-based systems draw on preexisting bodies of information.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly, Peer Reviewed & Referred Journal|

| Volume 5, Issue 12, December 2022 |

| DOI:10.15680/IJMRSET.2022.0512027 |

Intelligent Beings

In a world where no one is in charge, software may function as an intelligent agent. It is able to adapt to its environment and keep moving on with its plans. They always have more than one strategy to reach their objectives. The ultimate objective of creating an intelligent agent is to enable it to learn all feasible actions and then choose the one that will get it closer to its goal. Agents with intelligence may learn and change to fit their surroundings.

Because it mimics human intellect, artificial intelligence can help identify and thwart cyberattacks. It is able to recognise patterns of behaviour that might be indicators of an impending assault. The application of machine learning in cyber defence may help identify and thwart assaults on industrial control systems. Cybersecurity systems can automatically thwart attacks by training machine learning models to detect suspicious activity that corresponds to specific attacks. The use of neural networks to identify suspicious activity in network traffic and other machine learning methods may greatly enhance intrusion detection systems.

Cybersecurity professionals use machine learning to identify and thwart assaults on industrial control systems. A cyber security system may prevent an automated attack by training machine learning models to detect suspicious activity that corresponds to a targeted assault. By adding machine learning to the anomaly detection system, anomaly detection technologies may be enhanced. Using data or anomalous machine learning models trained on that data, anomalous behaviour may be detected using machine learning. The four main parts of an anomaly detection method are input, training data, model parameters, and output. The goal of these systems is to use machine learning as a metric to identify any suspicious activity in network traffic and then either filter it out or take some other action if necessary. An unusual occurrence is anticipated based on a series of observations, which serves as the input. This may be anything from the IP addresses of a company's edge routers to the numbers of TCP ports or HTTP header data. System annotations are stored in the training data, which is a set of observation sequences. It is probable that these sequences include singular occurrences. Model parameters such as normalisation parameters, detection threshold, and anomaly detection sensitivity determine the training method. These determine whether an anomaly detector is overconfident or underconfident in its ability to detect an occurrence. How the anomaly detector handles false positives is also defined by the model parameters. Lastly, a hypothesis generator and a confidence level are the results of an anomaly detector. Confidence is a measure of the probability that an unusual occurrence is happening in a certain order. Anomaly detectors employ hypotheses, which are potential explanations for the occurrence, to search for patterns in the data.

4.2 Countering Cyberthreats from an AI Perspective

Our current methods of combating cybercrime are antiquated, but artificial intelligence (AI) applied to the problem of malware detection and identification could soon be obsolete. Significant security improvements may be achieved by using AI to detect harmful files prior to their access to the end user. Malware detection has made extensive use of several AI/ML methods, with varying degrees of success [19]. One method searches for malware source code repositories using a technique called "SourceFinder" and examines them based on attributes and characteristics [30]. This strategy makes use of machine learning and data mining. Machine learning is another approach that may be used to categorise files based on the presence or absence of certain strings that may signal the existence of malware [34]. One alternative is to use AI and ML to identify potentially harmful patterns in binary executable files [32] [32]. Another way to find and halt malware is to use a self-organising network that changes over time using visual binary patterns found in the code [5].

By sifting through massive data sets in search of suspicious patterns, systems often use heuristics, the act of searching for patterns in data, to detect malware documents that might potentially indicate the existence of malicious software. That is to say, computers may look for recently updated files by analysing their hash values, or they can notice that a new file is excessively huge by analysing its size metrics over time. Heuristics like pattern matching, statistical analysis, and mimicking known malware signatures are included into antivirus (AV) programs.

The Byte-activation analysis neural network type, introduced by Coull et al. [9], maps the activation of each byte to the response to an input. In contrast, FireEye[20] constructed three networks using the Convolution neural network, each with its own unique combination of parameters including training set sizes and dropout settings. At some point along the process, dropout could have been enabled or disabled. In order to determine the exact parameters, the networks were trained using a specific dataset consisting of 7 million files. Inputs with tiny, undetectable differences that induce neural networks to incorrectly report them are known as adversarial examples. This kind of assault is the subject of the study by Demetrio et al. [10], which focusses on neural networks that are supposed to automatically identify malware. This network's goal is to examine the structure and try to question it by creating adversarial instances that are misclassified. Previous research used a similar strategy, however this study's findings vary from those of [22] and [23].

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly, Peer Reviewed & Referred Journal|

| Volume 5, Issue 12, December 2022 |

| DOI:10.15680/IJMRSET.2022.0512027 |

Additionally, Bose et al. [7] demonstrates that their method may enhance understanding of each categorisation from [9] [10], and they also hunt for greater performance by investigating new regions of solutions. Filter A is responsible for detecting goodware material, while Filter B is responsible for identifying which elements of a file are harmful. These two filters are part of the architecture.

Code obfuscation is a method that sophisticated malware uses to avoid detection by anti-malware programs that rely on signature-based approaches. To address this, Sharma et al. [33] presents a novel technique that use Fisher Score for feature selection and five classifiers to discover unknown harmful software, drawing on an approach they employed to increase the accuracy of de-tection of unknown sophisticated malware. Among other significant works in the same genre, there is a study on malware classification and detection using data mining and machine learning published by Chowd-hury et al. [8]. They categorise harmful websites that might infect users via various approaches. In their study, Hashemi et al. [18] used KNN and SVMs algorithms to identify suspicious malware in the data. The use of a deep convolutional neural network (CNN) to detect malware in Android devices was described in [26], while a new ML method known as rotation forest was described in [40]. The SAE model for intelligent malware detection is based on analysing Windows API calls, and it was presented by Ye et al. [39] as a novel deep learning model. Results from experiments demonstrate that this strategy outperforms and improves upon conventional shallow learning for malware identification.

Using AI to analyse message content and search for patterns characteristic of spam is one way to identify spam. A big number of machine learning algorithms trained on real-world data sets are used to do this.

A variety of communications, both spam and not. Oftentimes, AI will take the place of humans in spam detection and can independently determine if messages are spam. Messages that the automated system suspects of being spam will first need to be reviewed by a human. One such system that was designed to filter out certain spam emails is the one that Feng et al. [13] showed. The naive Bayes method and the support vector machine were integrated.

However, there is a growing trend towards using AI for spam detection in online review verification. For example, Lau et al. [38] created a novel unsupervised text mining model to investigate the potential of identifying inauthentic reviews. After being compared to supervised learning methods—which have previously achieved success in the review industry—this approach was trained on a semantic language model to detect review duplication. Using a higher-level idea of association, the dataset was trained. The data were analysed in order to derive reviewers' and postings' knowledge of context-sensitive concept associations.

By comparing the email's content to a database of previous phishing emails, the Phishing detection system may identify these malicious emails [4] [29]. Also, if the sender is trying to impersonate someone else, the system will be able to tell. Additionally, the phishing detection system is compatible with audio, video, and picture communications. Either sending or receiving an email with sensitive information triggers the system's activation. The present phishing detection system includes characteristics such as:

Phishing schemes sent over email are identified automatically.
- The quarantine folder is used to store emails that contain dangerous material.
- Notifies the user when the system identifies a new email virus.
- Thorough records of every email correspondence
— Identifies emails that may include malicious links
- Produces a report for each identified email automatically.

The phishing detection system's main objective is to identify and redirect emails that include malicious links. The use of a neural network in conjunction with the Monte Carlo algorithm and a risk-minimization strategy allowed Feng et al. [12] to identify phishing websites. Mahajanet al. [25] offered an alternative method for detecting phishing websites using machine learning algorithms; their system would distinguish between genuine and malicious URLs based on a number of characteristics. In order to circumvent the shortcomings of blacklist and heuristic-based approaches—which are unable to identify phishing attacks—they use ML techniques to identify phishing URLs.

The use of artificial intelligence to intrusion detection systems is a very young and exciting area of study. Cyber threat intelligence is a subfield of computer science concerned with creating smart systems to identify, categorise, and counteract cyber threats.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly, Peer Reviewed & Referred Journal|

| Volume 5, Issue 12, December 2022 |

| DOI:10.15680/IJMRSET.2022.0512027 |

In order to prevent harm, they seek out harmful activity and halt it before it happens. You may use it on its own or integrate it with other security software, like antivirus, to make it even more effective. Commonly, an intrusion detection system's ruleset specifies what actions, such sending an excessive number of messages in a specified time frame or email subject lines containing certain terms, are considered attacks. After that, the IDS checks these rules against each data packet and acts accordingly. Typically, an intrusion detection system is set up to notify users if it detects anything that may be a sign of an assault or attempt at an incursion. There are primarily two kinds of IDS responses: active defences and passive defences. Active defences include an IDS initiating a reaction. In the event of a possible incursion attempt, for instance, it might notify the on-duty staff. Instead of waiting for a report from another system, an active defence begins an action at the moment of detection, making it the closest to a "real-time" defence. In a passive defence, the intrusion detection system (IDS) does not take any action until it receives and processes the signal that an intrusion attempt has occurred. When an on-premises system detects changes in the network traffic surrounding its perimeter, it may trigger this kind of reaction by sending a report to a central monitoring hub and saving the data in an analytics database.

In order to decrease the amount of false alarms that occur when attempting to detect an intruder, an AI-based system seeks to optimise certain attributes and enhance its classifiers. It may also aid in identifying and responding to security threats in an organization's environment as soon as they are discovered. An intrusion detection system was developed by Al-Yaseen et al. [3] using a mix of support vector machines (SVM) and a modified k-means. In contrast, to identify any network abnormality, Hamamoto et al. [16] used fuzzy logic in conjunction with a genetic algorithm. The goal was to foretell the flow of data over a network during a certain time frame.

Using a comprehensive literature review, the authors of [17] conclude that Hybrid Machine Learning approaches have been extensively used in intrusion detection efforts over the last several decades. An architecture that combines audit data mining with anomaly detection and abuse detection was suggested by Barbara et al. [6]. The Self Adaptive Bayesian Algorithm, developed for use with massive datasets, was utilised by Farid et al. [11] to enhance anomalous intrusion detection. When deciding which features to use, another method was Correlation-Based Feature Selec-tion. It improved the reduced dataset's detection rate by selecting the optimal feature set and removing irrelevant datasets [15]. A novel method for decreasing data dimensionality was been up by Chowdhury et al. [24]. Their method for data visualisation and calculation is based on triangles rather than a conventional neural network.

V. CONCLUSION

Thanks to AI, even with few resources, cyber attacks may be detected and stopped in real-time. Cyberattacks are dynamic and ever-changing, making it difficult for humans to gather intelligence at a rapid pace. Machine learning, however, allows AI to devour data for rapid analysis and provide top-notch security coverage without diverting resources from ongoing projects. Machine learning frees up human analysts to think of creative ways to combat cybercrime and understand the findings of deep analysis.

AI won't solve every security problem. There are still gaps in cybersecurity prevention and repair offered by AI-based solutions, despite their widespread and decreasing costs in most areas. Artificial intelligence has its limitations when faced with an unwavering human opponent. Keep in mind that AI isn't a factotum and can't (or won't) do everything by itself just yet. If you want it to become better over time, you need invest in human training and supervision. From what we can see, AI has had a net beneficial effect on cybersecurity and associated concerns. As a result, future advancements in AI and ML will propel cybersecurity to a whole new level of sophistication.

REFERENCES

1. Cybersecurity Ventures. (2022). *Official annual cybercrime report*. Retrieved May 19, 2022, from https://cybersecurityventures.com/annual-cybercrime-report-2017/
2. World Economic Forum. (2022). *Global cybersecurity outlook 2022*. Retrieved May 19, 2022, from https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf
3. Al-Yaseen, W., Othman, Z., & Ahmad Nazri, M. Z. (2017). Multi-level hybrid support vector machine and extreme learning machine based on modified k-means for intrusion detection system. *Expert Systems with Applications, 67,* 1–10. https://doi.org/10.1016/j.eswa.2016.09.041
4. Banu, R., M., A., C., A., S., A., Ujwala, H., & N., H. (2019). Detecting phishing attacks using natural language processing and machine learning. In *Proceedings of the International Conference on Communication and Electronics Systems* (pp. 1210–1214).

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly, Peer Reviewed & Referred Journal|

| Volume 5, Issue 12, December 2022 |

| DOI:10.15680/IJMRSET.2022.0512027 |

5. Baptista, I., Shiaeles, S., & Kolokotronis, N. (2019). A novel malware detection system based on machine learning and binary visualization. In *Proceedings of the International Conference on Communications Workshops (ICC)* (pp. 1–6). https://doi.org/10.1109/ICCW.2019.8757060
6. Barbara, D., Couto, J., Jajodia, S., Popyack, L., & Wu, N. (2001). ADAM: Detecting intrusions by data mining. In *Proceedings of the IEEE Workshop on Information Assurance and Security* (pp. 5–6).
7. Bose, S., Barao, T., & Liu, X. (2020). Explaining AI for malware detection: Analysis of mechanisms of MalConv. In *Proceedings of the 2020 International Joint Conference on Neural Networks (IJCNN)* (pp. 1–8).
8. Chowdhury, M., Rahman, A., & Islam, M. R. (2018). Malware analysis and detection using data mining and machine learning classification. In *Proceedings of the Advances in Intelligent Systems and Computing* (pp. 266–274). https://doi.org/10.1007/978-3-319-67071-3_33
9. Coull, S., & Gardner, C. (2019). Activation analysis of a byte-based deep neural network for malware classification. In *Proceedings of the IEEE Symposium on Security and Privacy Workshops* (pp. 21–27). https://doi.org/10.1109/SPW.2019.00017
10. Demetrio, L., Biggio, B., Lagorio, G., Roli, F., & Armando, A. (2019). Explaining vulnerabilities of deep learning to adversarial malware binaries. *arXiv preprint arXiv:1901.03583.*
11. Farid, D., & Zahidur Rahman, M. (2010). Anomaly network intrusion detection based on improved self-adaptive Bayesian algorithm. *Journal of Computers, 5*(1), 23–31.
12. Feng, F., Zhou, Q., Shen, Z., Xuhui, Y., Lihong, H., & Wang, J. (2018). The application of a novel neural network in the detection of phishing websites. *Journal of Ambient Intelligence and Humanized Computing.* https://doi.org/10.1007/s12652-018-0947-2
13. Feng, W., Sun, J., Zhang, L., Cao, C., & Yang, Q. (2016). A support vector machine-based naive Bayes algorithm for spam filtering. In *Proceedings of the International Conference on Data Mining and Big Data* (pp. 1–8).
14. Guan, Z., Li, J., & Wu, L. (2017). Achieving efficient and secure data acquisition for cloud-supported Internet of Things in smart grid. *IEEE Internet of Things Journal, 4*(6), 1934–1944.
15. Hall, M. (2000). Correlation-based feature selection for machine learning. *Department of Computer Science Technical Report, 19.*
16. Hamamoto, A., Carvalho, L., Sampaio, L. D. H., Abrão, T., & Proença, M. (2017). Network anomaly detection system using genetic algorithm and fuzzy logic. *Expert Systems with Applications, 92,* 390–402.
17. Hamid, Y., Muthukumarasamy, S., & Ranganathan, B. (2016). IDS using machine learning: Current state of art and future directions. *British Journal of Applied Science and Technology, 15,* 1–22.
18. Hashemi, H., Azmoodeh, A., Hamzeh, A., & Hashemi, S. (2017). Graph embedding as a new approach for unknown malware detection. *Journal of Computer Virology and Hacking Techniques, 13*(3), 109–123. https://doi.org/10.1007/s11416-016-0278-y
19. Hossain Faruk, M. J., Shahriar, H., Valero, M., Barsha, F., Sobhan, S., Khan, A., Whitman, M., Cuzzocrea, A., Lo, D., Rahman, A., & Wu, F. (2021). Malware detection and prevention using artificial intelligence techniques. In *Proceedings of the IEEE International Conference on Big Data (Big Data)* (pp. 4410–4419). https://doi.org/10.1109/BigData52589.2021.9671434
20. Johns, J. (2017). *Representation learning for malware classification*. Retrieved May 19, 2022, from https://www.fireeye.com/content/dam/fireeye-www/blog/pdfs/malware-classification-slides.pdf
21. Kissell, R. L. (2021). Chapter 2 - Algorithmic trading. In R. L. Kissell (Ed.), *Algorithmic trading methods (Second Edition)* (pp. 23–56). Academic Press. https://doi.org/10.1016/B978-0-12-815630-8.00002-8
22. Kolosnjaji, B., Demontis, A., Biggio, B., Maiorca, D., Giacinto, G., Eckert, C., & Roli, F. (2018). Adversarial malware binaries: Evading deep learning for malware detection in executables. *arXiv preprint arXiv:1803.04173.* https://doi.org/10.48550/ARXIV.1803.04173
23. Kreuk, F., Barak, A., Aviv-Reuven, S., Baruch, M., Pinkas, B., & Keshet, J. (2018). Deceiving end-to-end deep learning malware detectors using adversarial examples. *arXiv preprint arXiv:1802.04528.*
24. Luo, B., & Xia, J. (2014). A novel intrusion detection system based on feature generation with visualization strategy. *Expert Systems with Applications, 41*(9), 4139–4147.
25. Mahajan, R., & Siddavatam, I. (2018). Phishing website detection using machine learning algorithms. *International Journal of Computer Applications, 181*(45), 45–47.
26. McLaughlin, N., Doupé, A., Ahn, G., Martinez-del Rincon, J., Kang, B., Yerima, S., Miller, P., Sezer, S., Safaei, Y., Trickel, E., & Zhao, Z. (2017). Deep Android malware detection. In *Proceedings of the ACM Asia Conference on Computer and Communications Security (AsiaCCS)* (pp. 301–308). https://doi.org/10.1145/3029806.3029823
27. Molina Valdiviezo, L., Furfaro, A., Malena, G., & Parise, A. (2015). A simulation model for the analysis of DDoS amplification attacks. *Simulation Modelling Practice and Theory, 54,* 40–51.
28. Obotivere, B., & Nwaezeigwe, A. (2020). Cybersecurity threats on the internet and possible solutions. *International Journal of Advanced Research in Computer and Communication Engineering, 9*(9), 92–97.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.54| Monthly, Peer Reviewed & Referred Journal|

| Volume 5, Issue 12, December 2022 |

| DOI:10.15680/IJMRSET.2022.0512027 |

29. Peng, T., Harris, I., & Sawa, Y. (2018). Detecting phishing attacks using natural language processing and machine learning. In *Proceedings of the International Conference on Big Data and Smart Computing* (pp. 300–301).
30. Rokon, M. O. F., Islam, R., Darki, A., Papalexakis, E., & Faloutsos, M. (2020). SourceFinder: Finding malware source-code from publicly available repositories in GitHub. *arXiv preprint arXiv:2010.04539.*
31. Sausalito, C. (2020). Cyberwarfare in the C-suite. Retrieved May 19, 2022, from https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
32. Schultz, M., Eskin, E., Zadok, F., & Stolfo, S. (2001). Data mining methods for detection of new malicious executables. In *Proceedings of the IEEE Symposium on Security and Privacy* (pp. 38–49).
33. Sharma, S., Challa, R., & Sahay, S. (2019). Detection of advanced malware by machine learning techniques. In *Proceedings of the International Conference on Intelligent Computing and Applications* (pp. 1–10).
34. Shrestha, P., Maharjan, S., Ramirez-de-la Rosa, G., Sprague, A., Solorio, T., & Warner, G. (2014). Using string information for malware family identification. In *Proceedings of the International Conference on Security and Cryptography* (pp. 686–697). https://doi.org/10.1007/978-3-319-12027-0_55
35. Syiemlieh, P., Golden, M., Khongsit, Sharma, U., & Sharma, B. (2015). Phishing - An analysis on the types, causes, preventive measures, and case studies in the current situation. *International Journal of Innovative Research in Advanced Engineering, 2*(1), 101–106.
36. Taghavi Zargar, S., Joshi, J., & Tipper, D. (2013). A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE Communications Surveys & Tutorials, 15*(4), 2046–2069.
37. Tandon, R. (2020). A survey of distributed denial of service attacks and defenses. *arXiv preprint arXiv:2008.01345.* https://doi.org/10.48550/ARXIV.2008.01345
38. Y. K. Lau, R., S. Y., L., Kwok, R. C. W., Xu, K., Xia, Y., & Li, Y. (2011). Text mining and probabilistic language modeling for online review spam detection. *ACM Transactions on Intelligent Systems and Technology, 2*(4), 1–30.
39. Ye, Y., Chen, L., Hou, S., Hardy, W., & Li, X. (2018). DeepAM: A heterogeneous deep learning framework for intelligent malware detection. *Knowledge and Information Systems, 54*(2), 1–21. https://doi.org/10.1007/s10115-017-1058-9
40. Zhu, H. J., You, Z. H., Zhu, Z., Shi, W. L., & Cheng, L. (2018). DroidDet: Effective and robust detection of Android malware using static analysis along with rotation forest model. *Neurocomputing, 272,* 638–646. https://doi.org/10.1016/j.neucom.2017.06.062

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com