Cyber Security Threat And Its Prevention Through Artificial Intelligence Technology

Rajashree Manjulalayam Rajendran[1], Bhuman Vyas[2]

[1]Lead Software Developer, HomeASAP LLC
[2]Senior Software Developer, Credit Acceptance Corporation

Abstract

Over the last decade, cyber threats have become a challenge for the proficient. Current security systems need more advancement to deal with exceptionally trained cybercriminals. Implementing Artificial Intelligence (AI) techniques helps detect scams but may bring other risks.

This research paper focuses on the intersection between cyber security threats and their forestallment using Artificial Intelligence (AI) technologies. It briefly outlines Artificial Intelligence (AI) applications for several cybersecurity crimes and estimates the probability of expanding cybersecurity by conservation of the defense mechanisms. The innovation of Artificial Intelligence has unlocked new room for the world's future. The methods to secure data have influenced the growth of Artificial Intelligence (AI) in cybersecurity.

The paper aims to establish awareness regarding the benefits of Artificial Intelligence (AI) technology and its assistance in protecting on a larger scale, i.e., in an organization or a business. The statistics mentioned in the paper are taken from valid sources and proved to favor the study. The study's implications can be used to promote the significance of Artificial intelligence (AI) in revolutionizing cyber security.

Keywords: Artificial Intelligence (AI), cyber security, cybercrimes, protection, revolutionizing, etc.

Introduction

A cyber security threat refers to malicious activities carried out by individuals with harmful intentions, aiming to cause disruption, damage, and chaos in cyberspace. Cybersecurity, on the other hand, encompasses the proactive actions taken to secure the vast realm of cyberspace, which includes information, data, and software, from all potential threats. As technology continues to advance, cybercriminals have become more creative and adept at evading traditional security measures. They constantly stay ahead of the game, making it increasingly challenging for individuals and organizations to effectively protect themselves from cyber threats.

In the modern era, the rise of cybercrimes poses significant risks and challenges that demand our immediate attention. Orthodox cybersecurity solutions have become insufficient at sensing and mitigating emergency cyberattacks. Developments in cryptographic and Artificial Intelligence (AI) techniques (in particular, machine learning) show potential in enabling cybersecurity specialists to counter the ever-evolving danger modeled by adversaries.

The accessibility of advanced technologies on the internet has surely revolutionized our lives. But it has also opened up new avenues for criminals to engage in acts of vandalism and commit various other crimes.

This has led to a serious increase in cybersecurity threats, and this requires unconventional and innovative solutions to maintain our safety and privacy.

In the 21st century, humans have made multiple revolutions in the field of cybersecurity to safeguard systems and networks from unforeseen threats. However, it is becoming increasingly evident that relying solely on human efforts has its limitations. No matter how sophisticated the security measures are, there will always be vulnerabilities that cybercriminals can exploit.

This paper intends to compare diverse approaches of artificial intelligence for fighting misconduct in cyberspace, or rather their application in systems for detecting and averting intrusions.

According to a statistics report, a 63% increase in cyber crimes was noticed in 2016, which showed a major rise compared to the previous year (Fig. 1). However, each year, a different threat demands unique solutions. As soon as the attackers access the system, they move laterally in search of high-profile targets from which they can ultimately exfiltrate intellectual property and data.

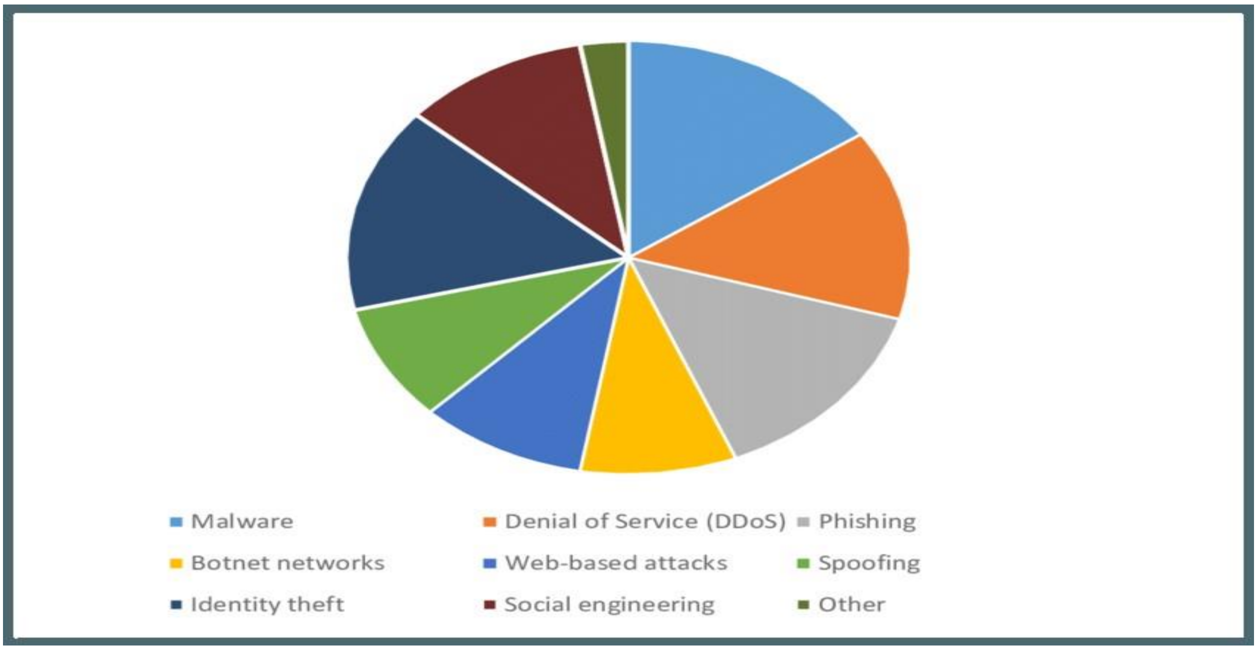

FIGURE 1. Different types of cyber attacks

To address this pressing issue, it is imperative to incorporate cutting-edge technologies and strategies into our cybersecurity arsenal. One of the most remarkable innovations in recent years is the advent of Artificial Intelligence (AI). AI offers a promising solution for analyzing massive amounts of data and identifying potential threats in real-time. By leveraging AI techniques and knowledge-intensive tools, we can significantly enhance our ability to detect, prevent, and respond to cyber-attacks.

With the stride in cyber-attacks, the human factor is not satisfactory for timely action. Intelligent agents carry out most system attacks, such as computer viruses and worms. Intelligent agents are autonomous computer-generated forces that can make conclusions or complete a service based on their environment, user input, and experiences (Fig. 2).

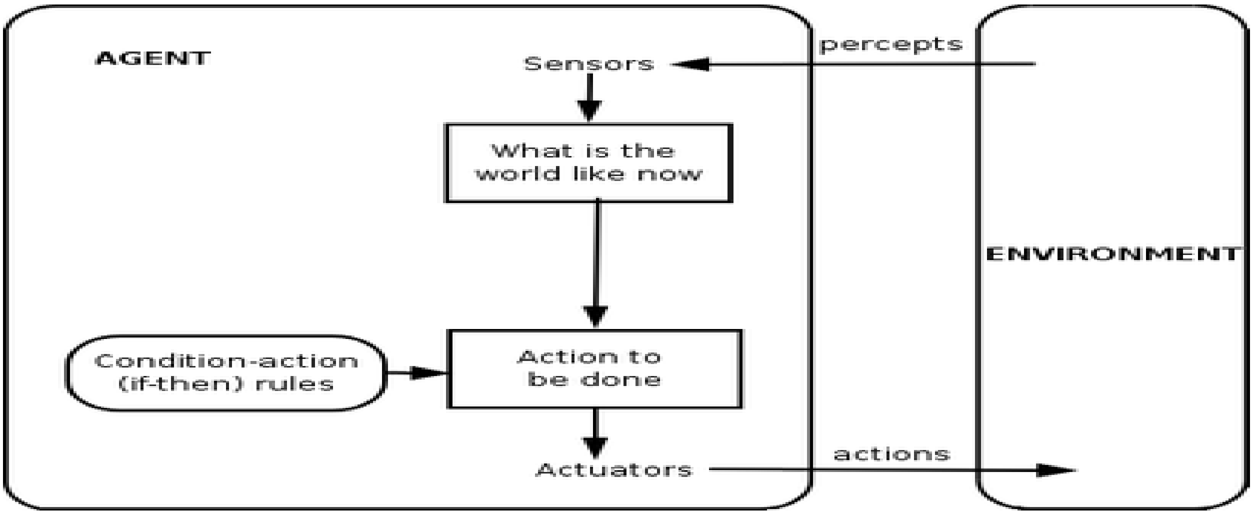

FIGURE 2. Simple Reflex agents

The integration of AI into cybersecurity practices not only improves protection but also enables efficient crisis management and response to network attacks. AI-powered systems can continually learn and adapt to emerging threats, ensuring that security measures remain effective even in the face of evolving cybercrime tactics. However, it is crucial to acknowledge that systems solely reliant on static algorithms may encounter challenges as new encounters emerge daily in the ever-evolving cyberspace.

Background

The idea to create a system beyond the horizons of human minds has been the goal for yesteryears. This idea has long been in action, chased by the most brilliant minds – researchers and innovators. Though there is always room for improvement, it looks like we have finally achieved it. However, it still requires protection and security from viruses that may corrupt it and the humans who may abuse it.

The need for a defensive system for technology became apparent when the first computer virus, known as the 'Creeper Virus,' was created in 1971 by Bob Thomas, widely recognized as the 'Father of Cyber Security.' The intention behind the virus was not to cause harm or adverse impact on the computers but rather to identify vulnerabilities in computer programs.

The invention of computers has signified the use of Artificial Intelligence (AI) to deal with all queries. Algorithms have been developed and advanced with the generation of computers. It is a fact that countries compete to get the best Artificial Intelligence (AI) technology for the improvement of their systems.

The term 'Artificial intelligence' was first invented by John McCarthy in 1956 as he held the first academic conference. The idea behind Artificial Intelligence (AI) was to design a machine that depicts human knowledge and expressions magnificently. This machine is a device or software that easily predicts the outcome and improves the accuracy of threat detection and response.

The primary purpose of integrating Artificial Intelligence (AI) technology is to identify all the threats that are not conceivable to human analysts. This can significantly reduce the number of cybercrimes and increase the efficiency of cybersecurity operations.

Artificial Intelligence (AI):

Artificial intelligence (AI) has revolved around how machines act or think in given circumstances. This universal definition comprises how closely machines can contemplate or act like humans. Spectrum on intelligence measures from acting like a human through the Turing test (Fig. 3). It is a method to inquire whether a computer is responding like a human. A computer communicating with a human is said to have intelligence when the human cannot distinguish whether the responses come from a computer or a human.

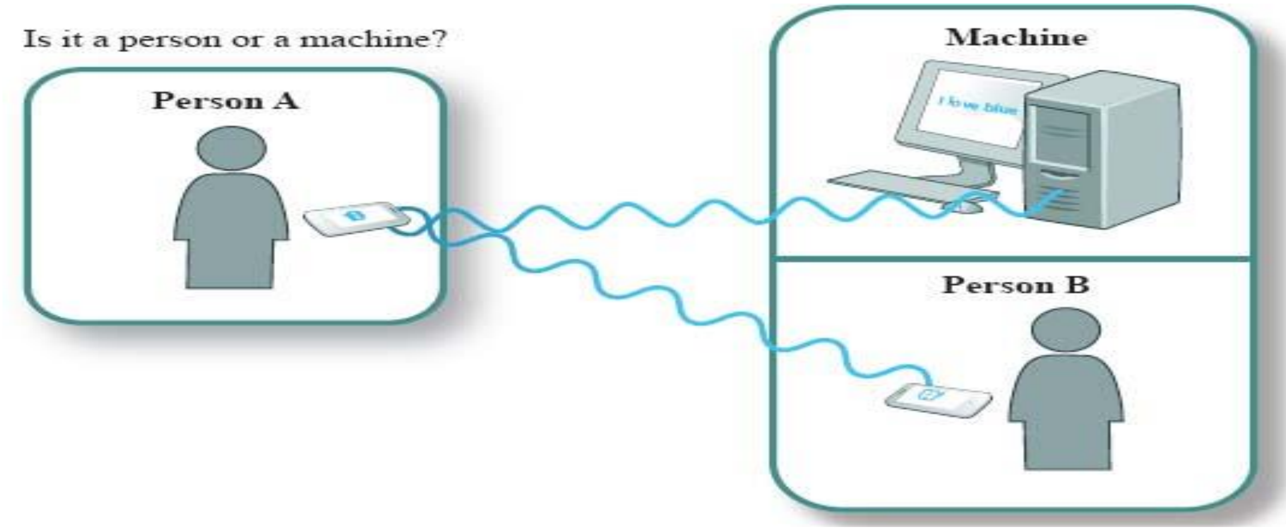

FIGURE 3. Turing test in Artificial Intelligence(AI)

The most pertinent use of Artificial intelligence (AI) technology in the cyberthreat landscape is in intrusion detection systems (IDS). An intrusion detection system IDS is a software application that scans a network for malicious activity or strategy violations(Fig. 4). Any breach is typically reported centrally by the system. Artificial intelligence (AI) can potentially analyze and classify a lot of internet traffic. Cybersecurity solutions based on Machine Learning (ML) technologies are used to automate the recognition of attacks and to improve their capabilities. Machine Learning (ML) solutions are used in intrusion detection systems (IDS). Machine learning (ML) techniques learn from the collected internet traffic to discriminate the malicious from the legitimate traffic class. It is the method of detecting malware networks and phishing emails. It uses algorithms and requires human intervention to correct errors.

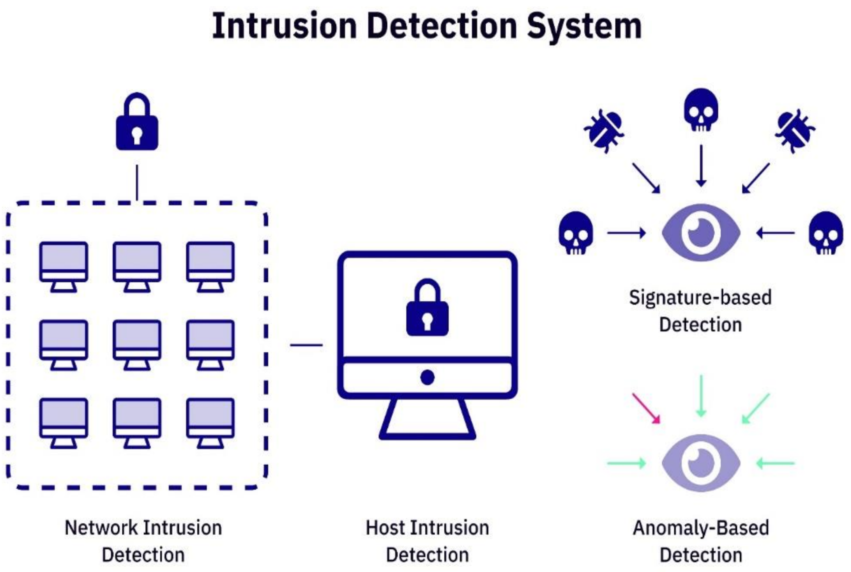
Intrusion Detection System
Signature-based Detection
Network Intrusion Detection
Host Intrusion Detection
Anomaly-Based Detection

FIGURE 4. Intrusion Detection System

Machine learning:

Conventionally, **machine learning** (ML) approaches can be classified into two groups: supervised and unsupervised learning. **Supervised machine learning** studies the relationship between labeled input and output training data. The samples are labeled according to their class (e.g., malicious or legitimate). In **unsupervised machine** learning, no data labeling or training is required. The nomenclature perspectives are converging, making it less essential to define machine learning algorithms based on whether they are supervised or unsupervised(Fig. 5).

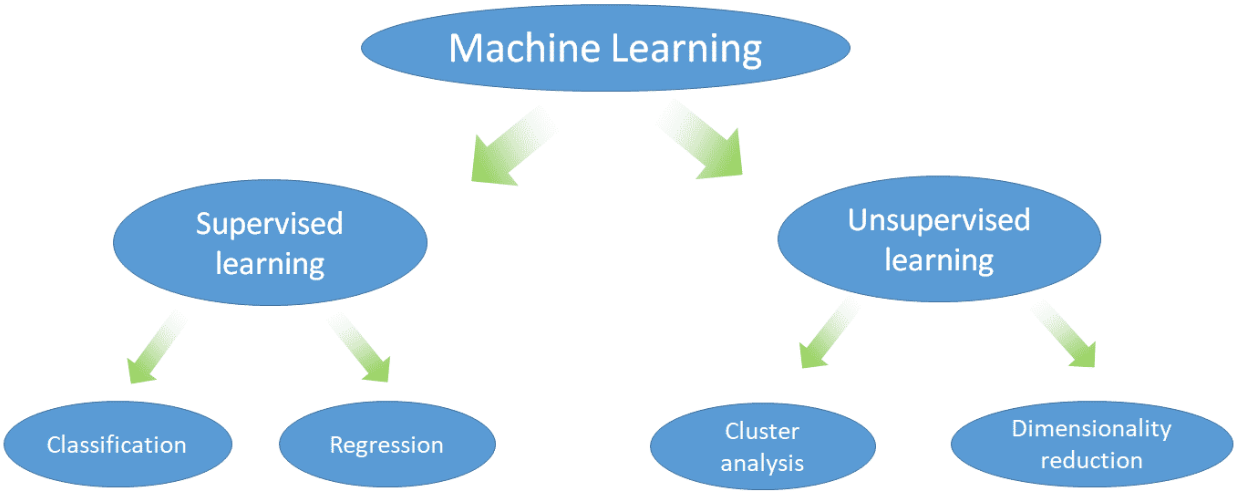

FIGURE 5. Machine Learning (Supervised & unsupervised)

Decision Tree:

A decision tree is a non-parametric supervised learning algorithm to create rules from training data samples. It has a hierarchical tree-like structure categorizes the data samples into many divisions. The figure below depicts a decision tree that starts with the root node(**Fig. 6). The root nodes branch into decision nodes. Based on the existing features, both node types conduct evaluations to form similar subsets denoted by leaf nodes. The leaf nodes signify all the probable conclusions within the dataset.

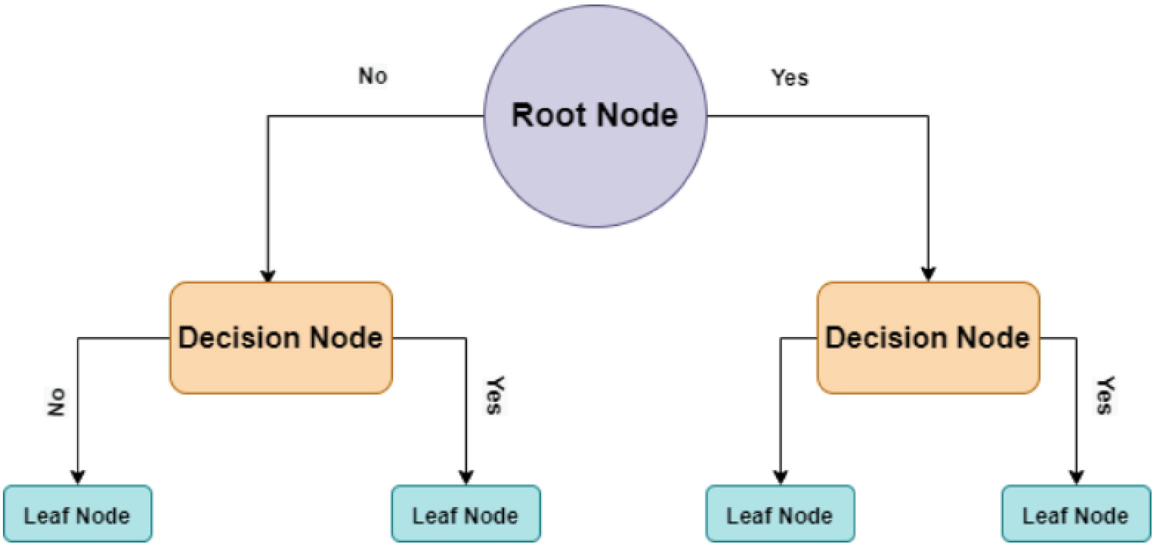

FIGURE 6. Decision Tree Algorithm in Machine Learning

The Artificial Neural Networks (ANNs):

Artificial Neural Networks (ANNs) are a subset of machine learning that is inspired by the mechanism of neurons working in the brain**(**Fig. 7). Artificial Neural Network (ANN) techniques model neurons in terms of a mathematical equation that reads a series of data samples to output a target value. The equation closely resembles the linear regression equation, where data characteristics of a sample are weighed to produce an output value.

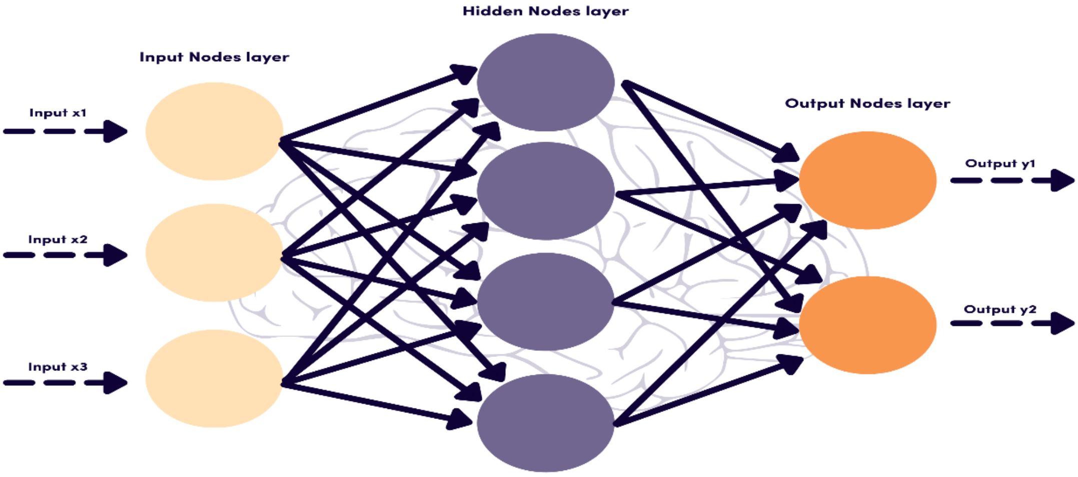

FIGURE 7. Artificial Neural Networks (ANNs)

K-Nearest Neighbors Algorithm:

The k-nearest Neighbor (KNN) algorithm is straightforward and simple, making it a prevalent choice in various realms. It relies on the clue that similar data points have similar labels or values. The k-nearest Neighbor (KNN) technique specifies data samples to create classes or clusters. It was first proposed as a non-parametric pattern analysis to determine the proportion of data samples in a neighborhood that yields a reliable approximation of a probability. The neighborhood was set as the k-number of data samples according to a distance metric. The votes from all K-neighbors decide how new data samples can be assigned to one of the clusters.

The K-Nearest Neighbor (KNN) algorithm is a popular machine-learning technique for classification and regression tasks. The KNN algorithm stores the entire training dataset as a reference during the training phase **(**Fig. 8). Then, it analyses the distance between the input data point and all the training examples. Next, the algorithm recognizes the K-nearest neighbors to the input data point based on their distances; the algorithm allocates the most common class label among the K-neighbors as the predicted label for the input data point. For regression, it estimates the average or weighted average of the target values of the K-neighbors to predict the value for the input data point.

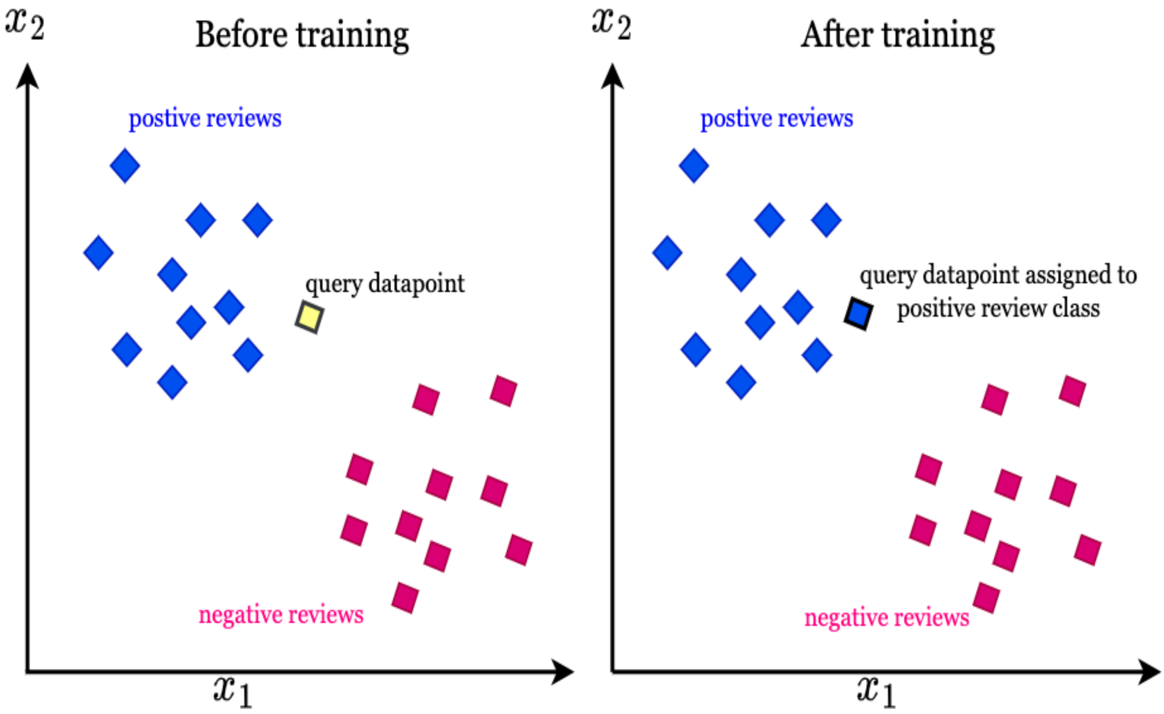

FIGURE 8. K-Nearest Neighbors Algorithm

The Role of Artificial Intelligence Technology in preventing Cybersecurity attacks:

The use of Artificial Intelligence (AI) technologies in government departments, industries, and companies has already been accomplished. Artificial Intelligence (AI) can save money and time by calculating and studying unidentified data, numbers, or patterns. The hackers are always one step forward as they seek new strategies to sabotage the system. Therefore, Artificial Intelligence (AI) technology helps to assess the possibility of a breach by inserting new defensive measures.

As stated previously, Artificial Intelligence (AI) has many benefits in different sectors and companies. The major advantage of Artificial Intelligence (AI) technology has been dealing with cyber security threats. Cyber security is the aspect of protecting systems from attacks through the internet. These attacks may leak confidential information and result in the loss of many resources. On a mass scale, these attacks cause terrorism in countries, which led to mass-scale destruction. Evaluating this situation, it is clear that Artificial Intelligence (AI) has become a main part of any organization. It has modified the dimensions of marketing, finance, and entertainment in every field. Robots mimicking humans, personal assistant applications, and devices have been developed for the ease of man. Alexa and Siri are the key examples.

To prove the importance of Artificial Intelligence (AI) in modern technology, multiple studies have been conducted after thorough research and investigations. There are several ways in which Artificial Intelligence (AI) can provide protection against malicious attacks. A few of them are discussed below.

1) Phishing Attacks:

Phishing is a tactic of manipulating or deceiving a person to steal personal data like login credentials and credit card numbers**(**Fig. 9). The hacker impersonates a reliable entity and compels the person to access a malevolent email or text. As soon as it opens, the hackers get access to all the systems that reveal confidential information, leading to fraud and forgery.

This considerable problem was solved by the invention of Artificial Intelligence (AI) as the leading company, *Darktrace,* came up with the solution to the problem. Artificial Intelligence (AI) helps to identify all the links and attachments that might cause jeopardy in the business. The *Antigena solution* is highly developed to recognize all phishing attacks.

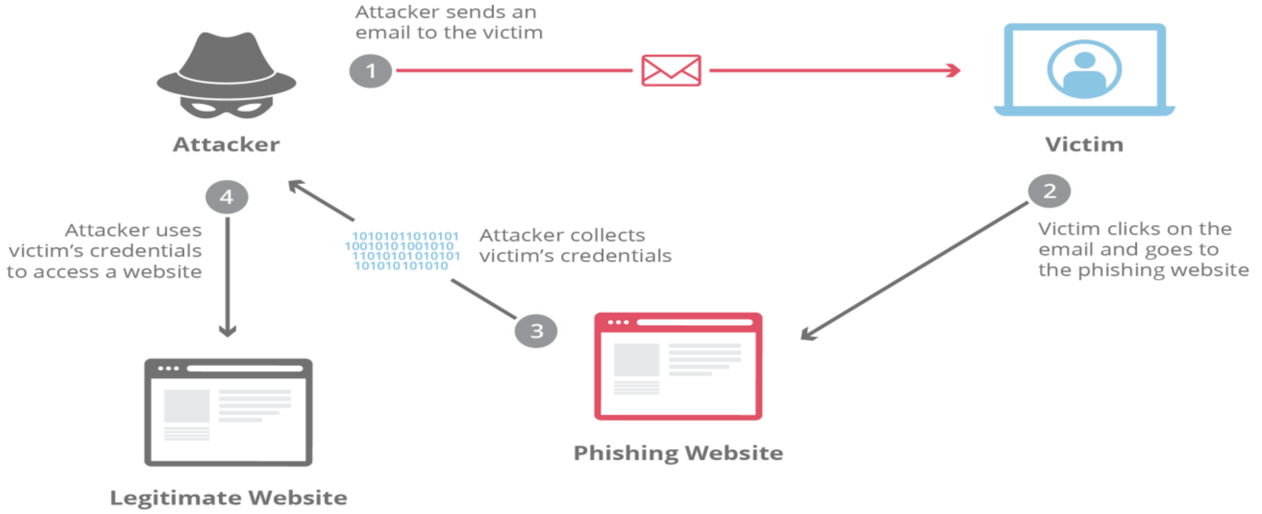
Attacker sends an email to the victim
1
Attacker
Victim
2
Victim clicks on the email and goes to the phishing website
4
Attacker uses victim's credentials to access a website
Attacker collects victim's credentials
3
Phishing Website
Legitimate Website

FIGURE 9. Phishing: Techniques & Mitigations

2) DNS Poisoning:

It is a highly misleading cyberattack where the culprits move the web traffic towards illegitimate websites instead of the intended one **(**Fig. 10). The user is usually unaware and often shares personal information that causes a problem.

This is a critical problem businesses face as there are more than *30,000* DNS poisoning attacks every day, and *70%* of all cyber-attacks include the DNS layer. To deal with the problem, DNS filters offer AI-powered DNS security. This filter helps to block fake and inappropriate websites.

DNS filtering is considered to provide edge-layer protection from all the security threats.

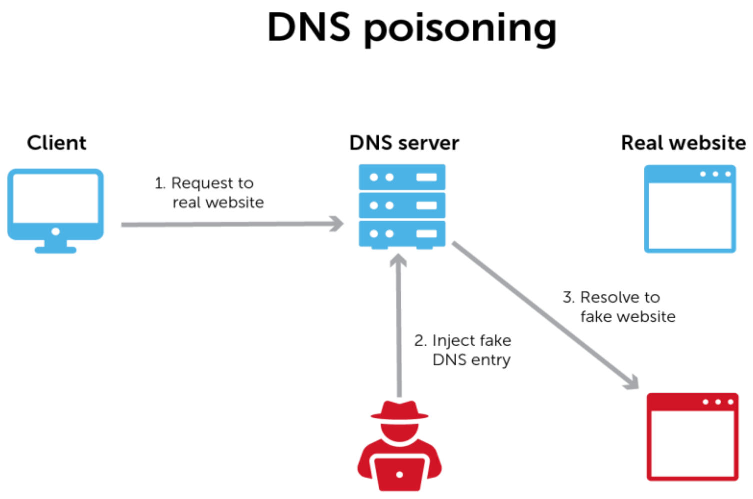

FIGURE 10. DNS poisoning

3) Breach Risk Prediction:

With the help of Artificial Intelligence (AI) technology, a company can work to enhance controls and improve an organization's cyber resilience. Artificial Intelligence (AI) software can predict the areas where there is a chance of breach and plan resources to deal with them accordingly **(**Fig. 11).

An American enterprise, *Sentinel One*, is a cybersecurity company that works on the above model. They detect a real-time threat and respond to it before it damages the organization. They deal proactively, which hinders the attackers from strategizing their plans.

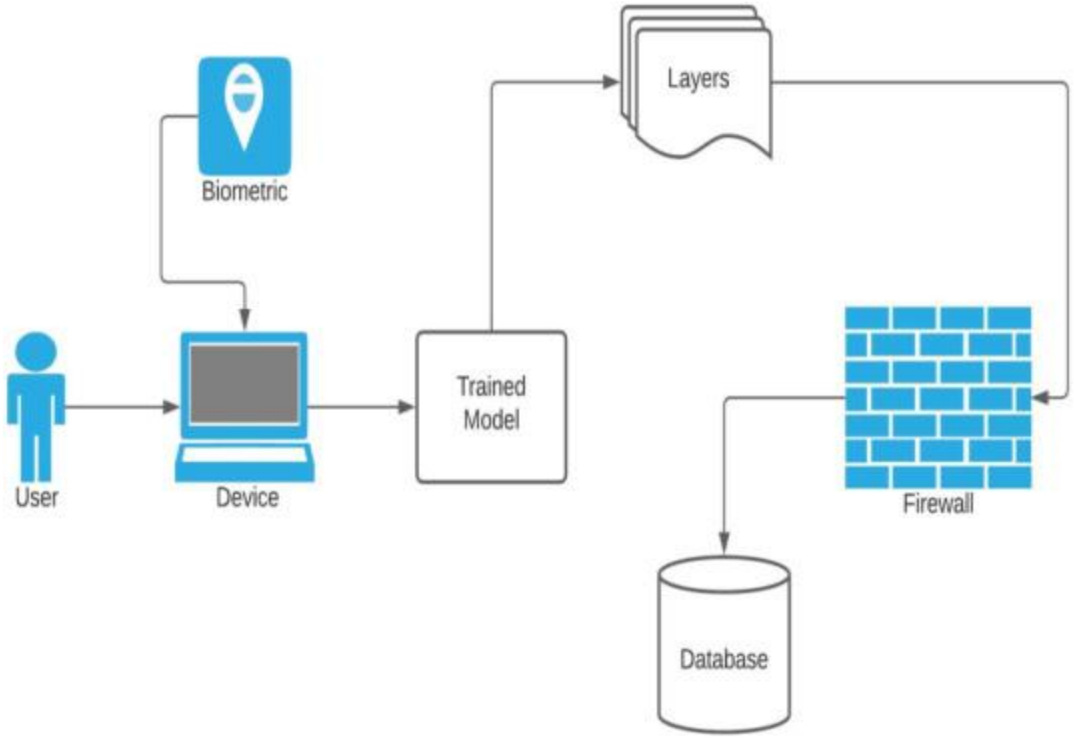

FIGURE 11. Security Breach Prediction using Artificial Neural Networks

4) Deep fakes identification:

The recent tool launched 'deep fake' has often been misused by several to manipulate someone else's face or videos. This has brought a lot of misguidance and chaos among people.

These tools are used deliberately to spread incorrect information from people with malicious intent. Their use can result in harassment and intimidation.

To counteract the problem, AI-based detection methods have been invented to detect fake images and videos. The algorithm needs to be trained before final usage. It is a two-step process where the video undergoes through some light image processing first. Then, in the second phase, it enters a Convolutional Neural Network (CNN) and a long short-term memory (LSTM) stage **(**Fig. 12).

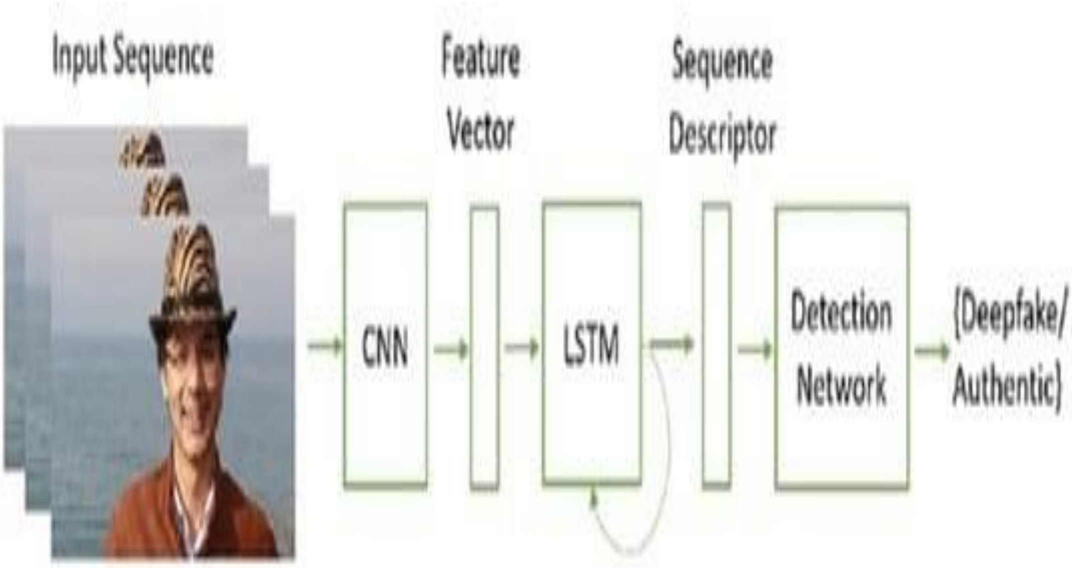

FIGURE 12. Deep Fake Detection using CNN and LSTM stage

5) Man-in-the-Middle (MITM) attacks:

In computer security, a man-in-the-middle attack is where the threat actor clandestinely relays and modifies the communications between two parties who think they are interacting directly with each other**(**Fig. 13). They potentially intercept the communication between two parties to use it for malicious purposes like making unauthorized buying or hacking.

One of the best practices is to have a secure internet connection to prevent attacks. Another solution is to use a VPN (Virtual Private Network). This encryption stops the MITM attack from infiltrating your network traffic.

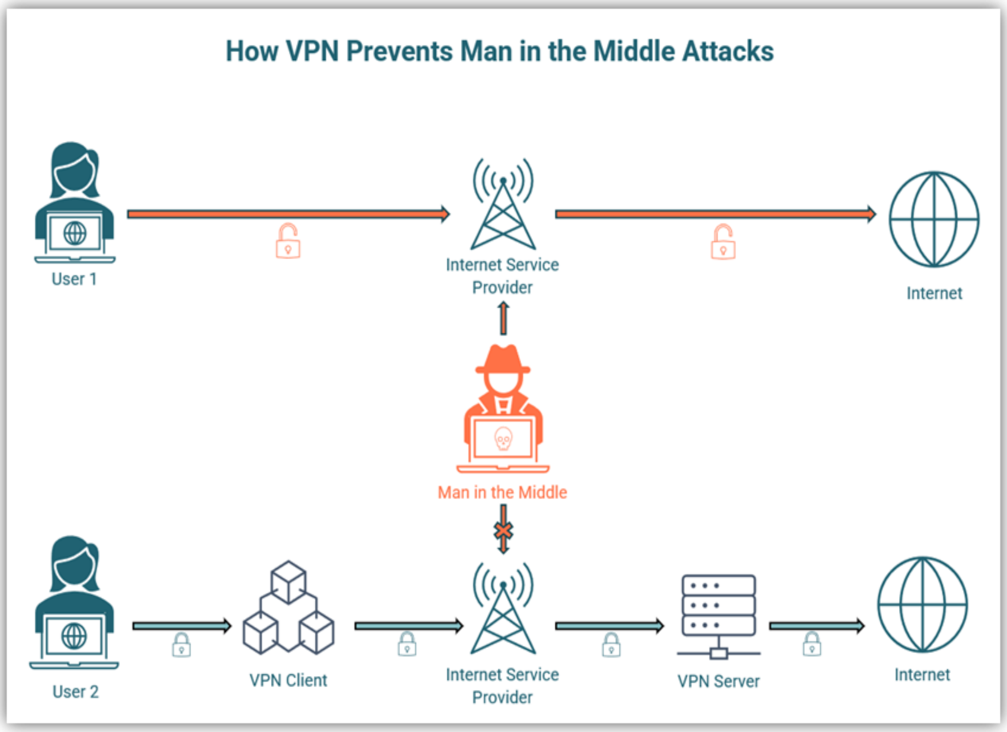
How VPN Prevents Man in the Middle Attacks
User 1
Internet Service Provider
Internet
Man in the Middle
User 2
VPN Client
Internet Service Provider
VPN Server
Internet

FIGURE 13. Man in the Middle Attacks

6) Denial of Service (DoS) attacks:

DoS (Denial of Service) attacks happen when a hacker overloads and crashes a server by overpowering it with many requests(Fig. 14). DoS attacks are increasingly becoming more sophisticated and harder to detect because of the ready availability of attacker tools.

Simple ways to fight DDoS/DoS cyber-attacks are to sieve traffic by region and protocol, detect flow anomalies, deploy dedicated DDoS mitigation, and update your disaster recovery plan with your client.

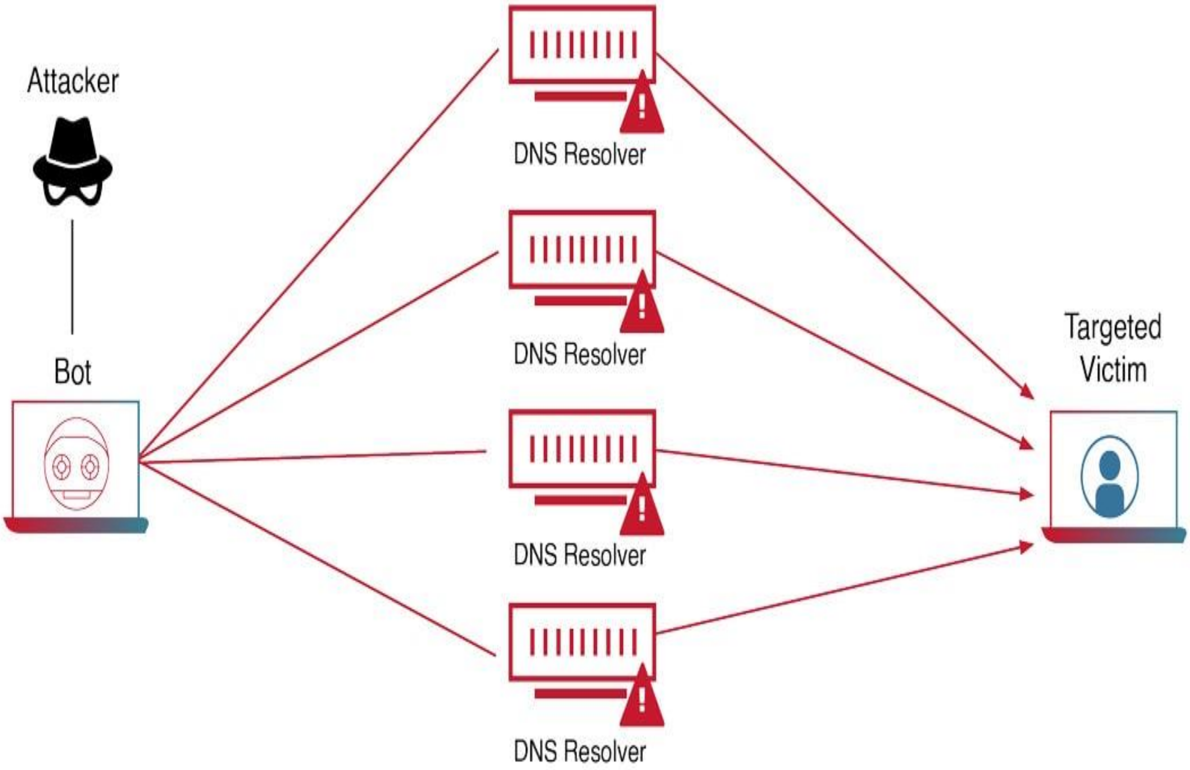

FIGURE 14. Denial of Service (DoS) attacks

7) Structured Query Language (SQL) injection attacks:

These cyberattacks exploit weaknesses in the SQL language by using vindictive SQL code for backend database manipulation to access information. This information may comprise any type of items, including confidential company data, user lists, or private customer details (Fig. 15).

SQL has a major impact on the running business. Suppose the attackers successfully access information that was not intended to be displayed. In that case, it may cause illegal viewing of the user list, deletion of entire data, or, in severe cases, lead to a detrimental loss in business.

The only way to prevent this bizarre cyber activity is to put authentication and confine the queries, including prepared statements. The developer must sanitize all input, not just web form inputs like login forms. They must eliminate possible malicious code, such as single quotes, and turn off the visibility of database errors on your production sites.

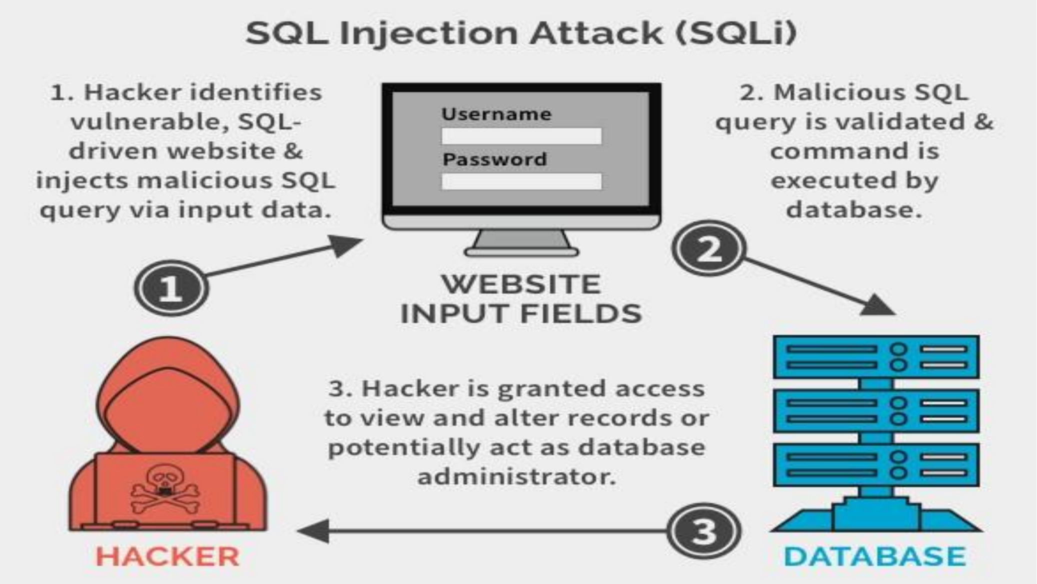
SQL Injection Attack (SQLi)
1. Hacker identifies vulnerable, SQL-driven website & injects malicious SQL query via input data.
Username
Password
WEBSITE INPUT FIELDS
2. Malicious SQL query is validated & command is executed by database.
1
2
3
3. Hacker is granted access to view and alter records or potentially act as database administrator.
HACKER
DATABASE

FIGURE 15. Structured Query Language (SQL) injection attacks:

8) Malware attacks:

This is one of the challenging difficulties that businesses often have to encounter. Introducing malware into a system can happen through numerous methods, including email attachments, malicious websites, or infected ones. Malware can decelerate computer performance by consuming system resources. Symantec’s 2016 threat report specifies that 78% of websites contain a critical vulnerability that, if exploited, may allow malicious code to be run without user interaction.

To keep up a website’s defenses, proper security controls such as web proxies, firewalls, and intrusion detection systems must be maintained. Malware protection and recognition can be strengthened without discouragingly impacting business output by using antiviral tools that can help against unforeseen viruses and worms(Fig. 16). The endpoint detection and response technology constantly looks out for any malware attacks and helps to provide protection. It is important to backup data regularly and repeatedly from endpoints and servers to allow for effective disaster recovery.

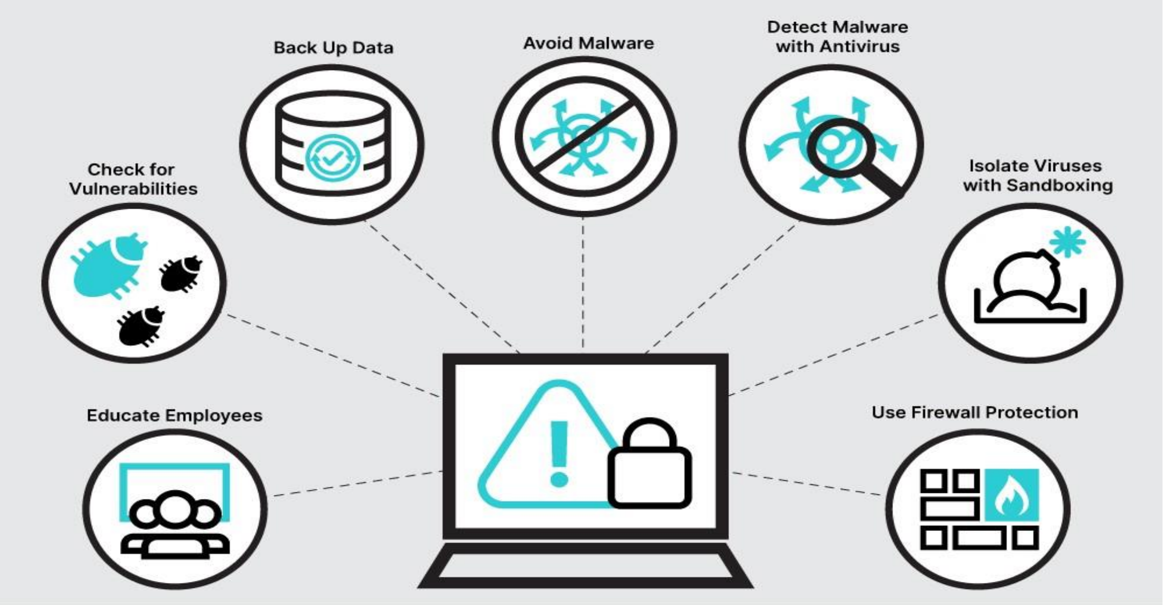
Back Up Data
Avoid Malware
Detect Malware with Antivirus
Check for Vulnerabilities
Isolate Viruses with Sandboxing
Educate Employees
Use Firewall Protection

FIGURE 16. Malware attacks

9) Password attacks:

Password attacks object to gain unofficial access to sensitive data and systems by compromising user passwords. The applications that use passwords as the only authentication factor are on the verge of password attacks because of the vulnerability.

The invader uses various methods to expose the credentials of a legitimate user, assuming their identity and privileges. The username-password combination is one of the oldest authentication techniques, so several approaches exist to obtain guessable passwords.

In a Brute force attack approach, the attackers use every possible password until the real one is found(Fig. 17). Usually, they start with the most generally used one that helps them to filter accounts in seconds. A specialized brute-force option is a dictionary attack, which restricts candidate passwords to words from the dictionary.

Another type is the keylogger, in which Hackers install software on a user's computer to record the user's keystrokes as they type the password.

To prevent the damage from this attack, it is wise to enforce strong password policies that assure users follow set criteria to prevent malicious actors from cracking their passwords. Other executions include the One-Time Password (OTP), biometric authentication, software tokens, and behavioral analysis.

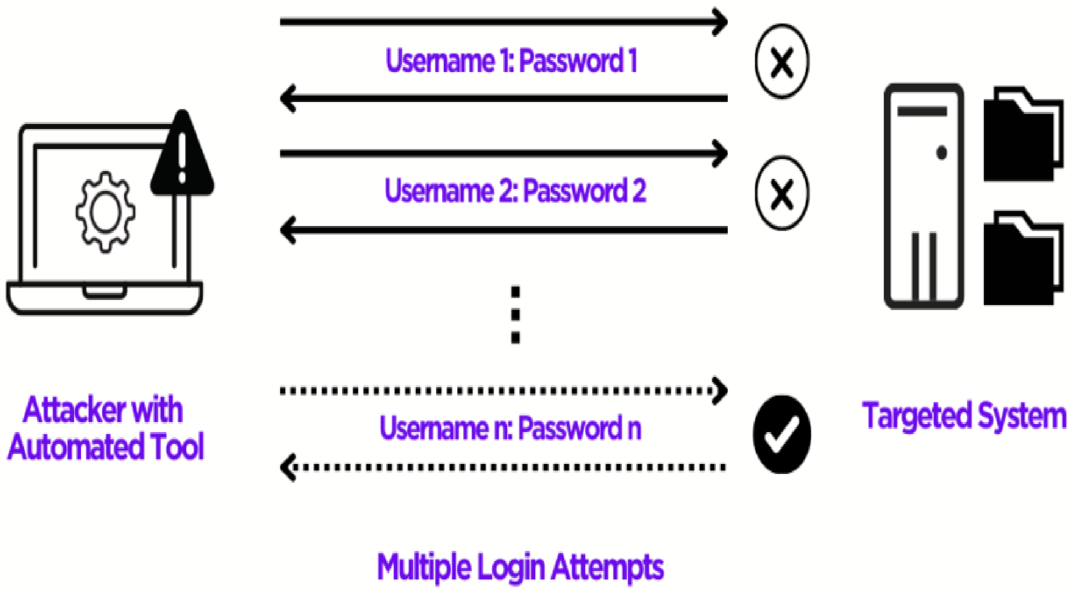

FIGURE 17. Password attacks

Results:

Artificial intelligence (AI) brings many benefits, but some risks come along. AI plays the role of a double-edged sword. The incorporation of AI in an organization can be a source of threat. The vulnerabilities in a system can be a potential threat to the system and a positive target for hackers. This is very common for regular users to be unaware of the system's security patches, which often leads to cyber-attacks and vulnerabilities for businesses.

Establishing regulations to reduce the widespread threat to cybersecurity is a complex task for policymakers. With the extensive use of AI, it has become easily accessible to anybody. As resourceful cybercriminals learn to use AI maliciously, they become a predominant threat. The easy availability of books and software allows hackers to learn new techniques to disrupt cyber security.

With the rise in speed and sophistication of attacks, AI has become an indispensable technology in the cybersecurity zone—the article emphasizes the increase in cyber threats and their complexities. We highlighted future risks of cybercrimes with a brief overview of their solutions.

Lately, proposed AI-based cybersecurity explanations have largely focused on machine learning techniques that use intelligent agents to differentiate between attack traffic and legitimate traffic.

The statistics are not inclusive, but the purpose is to outline the cyber threat landscape.

During 2016, the level of attacks was quite similar to the last year. However, a peak was experienced in the central months. Starting from September 2015, it registered a more steady activity until December, when 2016 experienced a new tail of events (Fig. 18).

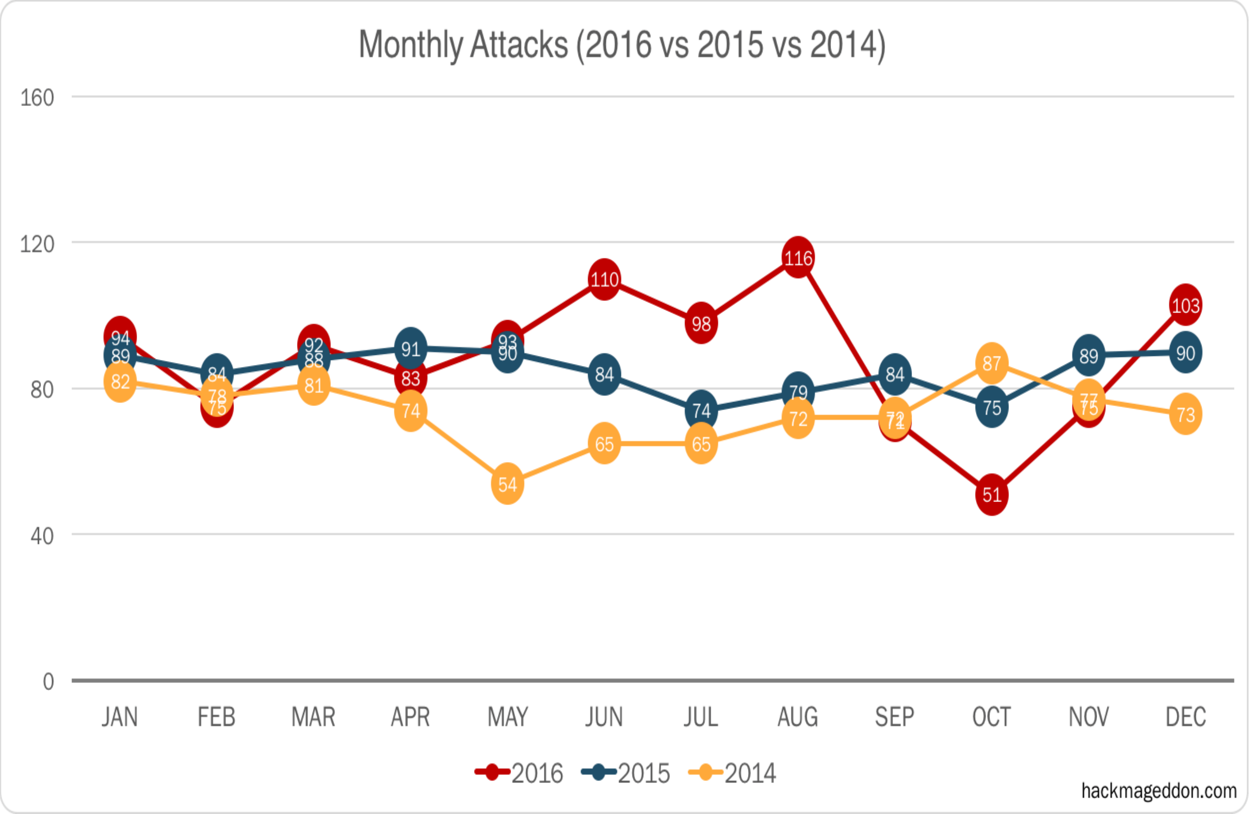

FIGURE 18. Graphic Representation showing comparative analysis in monthly attacks of (2016 vs. 2015 vs. 2014)

There has been an increase in connectivity worldwide over the last decade. It has become mandatory to carry a device to stay linked all the time. The internet remains evolving in terms of the number of users, its size, heterogeneity of devices, and the type of applications that are developed for the ease of mankind. Today, similar to electricity, water, and gas, the Internet has become a significant utility in the daily lives of people around the world. As more devices connect to the internet, it is susceptible to more attacks by cybercriminals.

Artificial Intelligence (AI) is a technology that allows machines to duplicate human behavior smartly. On the other hand, the Internet of Things (IoT) is referred to as a network of devices and sensors that are connected to the internet. The growth of IoT devices over the past few years is illustrated in the graph below(Fig. 19).

AI and IoT are the two sets of dynamic technologies that are changing quickly. These two technologies are bringing transformation to the world of business. It has surely impacted consumer psychology, from managing inventories to improving personalized shopping experiences. Both inventions have revolutionized the way of dealing in the business. IoT analytics helps many companies improve the performance and delivery of better outcomes.

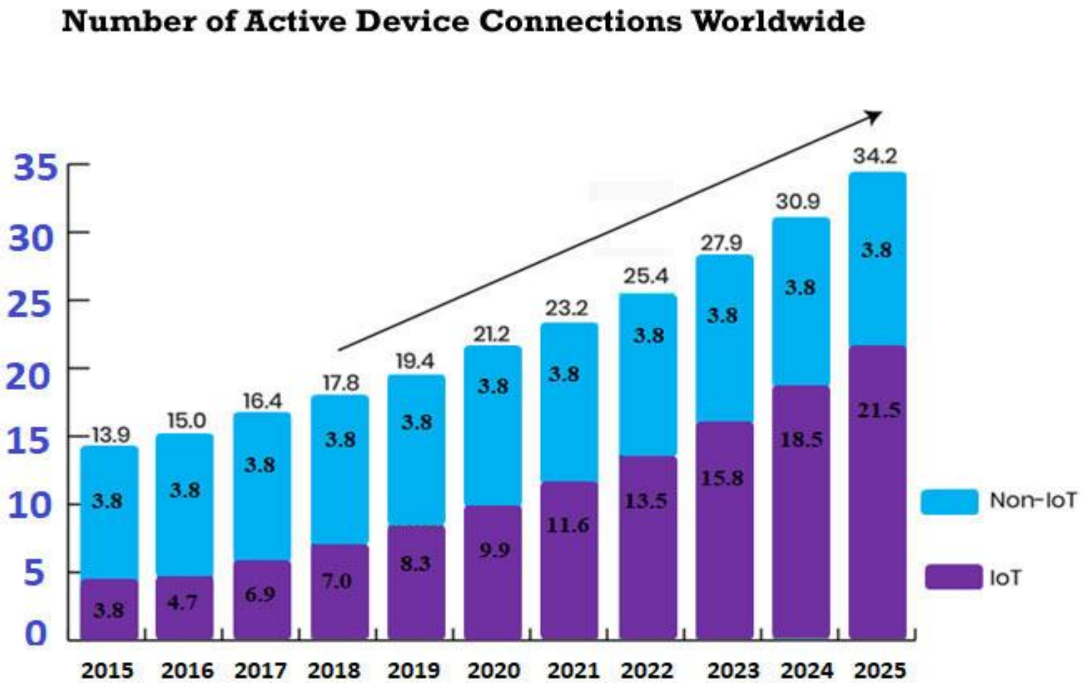

FIGURE 19. Graphic representation showing an increase in IoT over the years

Although AI's role in cracking cybersecurity issues continues to be inspected, some fundamental apprehensions surround where AI deployment can become regulated. For example, as machines become imperative solutions for humanity, these will consume fundamental resources for life increasingly. When humans and machines strive for scarce resources, a new form of domination will propagate. This, in turn, will provoke a new research avenue.

Conclusion

Modern problems require modern solutions. AI's invention for humankind's benefit has proven to be the best discovery of the century. The advantages of Artificial Intelligence (AI) have shadowed the flaws that come along from its misuse. The above articles prove that the scams offered by the attackers can only be dealt with through Artificial Intelligence (AI). Artificial Intelligence (AI) software in cyber security helps in early detection of problem that avoids later impairment.

The field of AI has vast options for researchers to explore. The Intrusion Detection and Prevention Systems research proves that Machine Learning is a technique that brings constructive results. Applying Machine Learning in IDPS systems reduces false positives and increases accuracy with the understanding to learn new threats. This causes cybercriminals to hide their intentions when probing networks and sending malware. Cybersecurity professionals need forceful policies to regulate AI in organizations so threats are less imminent.

AI allows growing autonomous computing solutions using the methods of self-control and self-configuration. Regarding the future of information security, AI is a promising area of research that focuses on improving cyberspace security. AI has undergone noteworthy variations over the last decade, with scientists progressing in the fight against cybercrime.

The recent development in Artificial Intelligence (AI) software helps detect online scams and frauds that can be a breakthrough for many cyber security organizations. The excellence of Artificial Intelligence (AI) in detecting threats and resolving them before human intervention has flabbergasted the world. Phishing detection with Artificial Intelligence (AI) technology has incredibly provided a haven for humans. Multiple Artificial Intelligence (AI) software has concealed the confidentiality of the user.

There is no doubt that cyber security threats are intimidating for any business. But with the developing breaches in the organization, the human source alone can't deal with it. Therefore, incorporating Artificial Intelligence (AI) technology with human involvement in an organization is key to staying protected and secure in a digital world.

With the help of Artificial Intelligence (AI) technology, organizations can probe cyber threats more hastily and effectively. This will enhance the security of the systems by bringing new modifications each time per the need.

References:

1. Anonymous. Father of Cybersecurity: Brief History, Contributions Explained [Internet]. Testbook. 2023. Available from: https://testbook.com/articles/father-of-cybersecurity#:~:text=Bob%20Thomas%20is%20a%20computer
2. Smith C, McGuire B, Huang T, Yang G. The History of Artificial Intelligence [Internet]. University of Washington; 2006 Dec. Available from: https://courses.cs.washington.edu/courses/csep590/06au/projects/history-ai.pdf
3. Mackay J. The Benefits And Challenges Of AI In Cyber Security [Internet]. www.metacompliance.com. 2023. Available from: https://www.metacompliance.com/blog/data-breaches/benefits-and-challenges-of-ai-in-cyber-security
4. Imperva. What is phishing | Attack techniques & scam examples | Imperva [Internet]. Imperva. 2023. Available from: https://www.imperva.com/learn/application-security/phishing-attack-scam/
5. Gray C. Five ways AI can be used to prevent cyber attacks [Internet]. aimagazine.com. 2022. Available from: https://aimagazine.com/ai-strategy/five-ways-ai-can-be-used-to-prevent-cyber-attacks

6. VanVliet S. What is DNS Poisoning? (aka DNS Spoofing) [Internet]. Keyfactor. 2021. Available from: https://www.keyfactor.com/blog/what-is-dns-poisoning-and-dns-spoofing/
7. Balbix. Using Artificial Intelligence in Cybersecurity | Balbix [Internet]. Balbix. 2018. Available from: https://www.balbix.com/insights/artificial-intelligence-in-cybersecurity/
8. Solinap M. Six Advantages Of Using SentinelOne [Internet]. SPK and Associates. 2022. Available from: https://www.spkaa.com/blog/six-advantages-of-using-sentinelone
9. Britt K. How are deepfakes dangerous? [Internet]. University of Nevada, Reno. 2023. Available from: https://www.unr.edu/nevada-today/news/2023/atp-deepfakes#:~:text=Typically%2C%20deepfakes%20are%20used%20to
10. Anonymous. Stopping deepfake news with an AI algorithm that can tell when a face doesn't fit [Internet]. spie.org. 2020. Available from: https://spie.org/news/stopping-deepfake-news-with-an-ai-algorithm-that-can-tell-when-a-face-doesnt-fit?SSO=1
11. Anonymous. AI in Cyber Security: Pros and Cons | Terranova Security [Internet]. terranovasecurity.com. 2023. Available from: https://terranovasecurity.com/blog/ai-in-cyber-security/
12. Anonymous. AI in Cybersecurity: Revolutionizing threat detection and defense | Data Science Dojo [Internet]. datasciencedojo.com. Available from: https://datasciencedojo.com/blog/ai-in-cybersecurity/
13. Calderon R. The Benefits of Artificial Intelligence in Cybersecurity [Internet]. 2019 Jan. Available from: https://digitalcommons.lasalle.edu/cgi/viewcontent.cgi?article=1035&context=ecf_capstones
14. Das R. Artificial Intelligence in Cyber Security. https://iopscience.iop.org/article/10.1088/1742-6596/1964/4/042072/pdf. 2021.
15. Ansari MF, Dash B, Sharma P, Yathiraju N. The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review [Internet]. papers.ssrn.com. Rochester, NY; 2022. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4323317
16. Dakov Yoshinov R. Increasing the level of network and information security using artificial intelligence. https://www.researchgate.net/profile/Georgi-Tsochev/publication/323919777_Increasing_the_level_of_network_and_information_security_using_artificial_intelligence/links/5c331bf5a6fdccd6b598b393/Increasing-the-level-of-network-and-information-security-using-artificial-intelligence.pdf. 2017.
17. Sheridan K. Major Cyberattacks On Healthcare Grew 63% In 2016 [Internet]. www.darkreading.com. 2016 [cited 2023 Dec 11]. Available from: https://www.darkreading.com/attacks-breaches/major-cyberattacks-on-healthcare-grew-63-in-2016
18. Zeadally S, Adi E, Baig Z, Khan I. Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity. IEEE Access. 2020;8:1–1. https://doi.org/10.1109/access.2020.2968045
19. Anderson I. The 12 Most Common Types of Cybersecurity Attacks Today [Internet]. https://blog.netwrix.com/. 2018. Available from: https://blog.netwrix.com/types-of-cyber-attacks
20. Anonymous. Top 5 Cyber Attack Types in 2016 So Far [Internet]. www.calyptix.com. 2016 [cited 2023 Dec 11]. Available from: https://www.calyptix.com/reports/top-5-cyber-attack-types-in-2016-so-far/
21. Passeri P. 2016 Cyber Attacks Statistics [Internet]. HACKMAGEDDON. 2017. Available from: https://www.hackmageddon.com/2017/01/19/2016-cyber-attacks-statistics/
22. Dilek S, Cakır H, Aydın M. Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review. International Journal of Artificial Intelligence & Applications [Internet].

2015;6:21–39. Available from: https://arxiv.org/ftp/arxiv/papers/1502/1502.03552.pdf

23. Izquierdo R. 5 Ways to Prevent Man-in-the-Middle (MITM) Attacks [Internet]. The Motley Fool. 2022. Available from: https://www.fool.com/the-ascent/small-business/endpoint-security/articles/mitm/
24. IBM. What is a Decision Tree | IBM [Internet]. www.ibm.com. Available from: https://www.ibm.com/topics/decision-trees#:~:text=A%20decision%20tree%20is%20a
25. Anonymous. 6 Types of Password Attacks [Internet]. OneLogin. 2019. Available from: https://www.onelogin.com/learn/6-types-password-attacks
26. Sengupta S. Password Attack - Definition, Types and Prevention [Internet]. crashtest-security.com. 2022. Available from: https://crashtest-security.com/password-attack/
27. Brucciani P. Why cyber security is so hard [Internet]. Medium. 2018 [cited 2023 Dec 11]. Available from: https://medium.datadriveninvestor.com/why-cyber-security-is-so-hard-fe05921a72a0
28. Acunetix. What is SQL Injection (SQLi) and How to Prevent It [Internet]. Acunetix. 2017. Available from: https://www.acunetix.com/websitesecurity/sql-injection/
29. Srivastava T. Introduction to KNN, K-Nearest Neighbors : Simplified [Internet]. Analytics Vidhya. 2019. Available from: https://www.analyticsvidhya.com/blog/2018/03/introduction-k-neighbours-algorithm-clustering/
30. Anonymous. Artificial Intelligence (AI) and Internet of Things (IoT) is Transforming the World [Internet]. iotdesignpro.com. 2020 [cited 2023 Dec 11]. Available from: https://iotdesignpro.com/articles/artificial-intelligence-ai-and-internet-of-things-iot-is-transforming-the-world-as-we-know-it