Name - Shreya Vilas Karade

Class – S.Y. MSc Computer Science

Subject – Research Methodology

Prn – 1132220617

Sr. No – 35

Assignment No – 1

Literature Review

Title

Use of Artificial Intelligence in Cyber Security using Machine Learning Algorithms and Malware Detection

Domain Area

Cyber Security

Problem Statement

Presently, the data in the companies, industries, government and also private data of many people is getting hacked or getting stolen or being changed. Because of this growing development in the IT field hackers, technocrats and geeks are getting smarter and smarter and are able to hack different hardcore layers of security. So, there is a huge need to get ahead of these people and for this Artificial Intelligence can help us. Artificial Intelligence is so powerful that it can be very useful to decrease these ongoing attacks.

Abstract

Nowadays cybersecurity breaches are increasing day by, even after applying layers of security. Also, the most prominent organizations/companies are facing security breaches and data is at huge risk. Different types of attacks like Phishing, Malware, Social Engineering, Ransomware and Advanced Persistent threats are taking place in huge numbers. On the contrary, today's security challenges are numerous. Cloud computing, social media, smart phones, and the widespread usage of numerous programmes such as WhatsApp and Viber have all posed significant security risks to users. To minimize the number of attacks Artificial Intelligence can be used. There are a huge number of challenges and procedures to overcome cyber-crimes. Cyber security systems that are based on the concept of Artificial intelligence will help to provide accurate and brief knowledge about all the industrial threats and in turn it will help us to make important decisions. AI has a huge demand in today's happening world so here we can use AI controlling the number of cybercrimes and decrease the number of attacks taking place.

AI and machine learning are now one of the most important elements to security of the IT sector as they have the necessary techniques and capabilities for the prevention of cyber-crimes. AI has many applications widespread in the cyber security solutions such as improving the overall security of digital systems, fraud detection, spot malware, monitoring swaths of data, and voice assistants.

We can define Artificial Intelligence as the scientific field that tries to understand and model human intelligence. There are certain threats that lead to severe destruction in the software. Malware can be considered one of them, it has the ability to spread autonomously though any defencelessness and carelessness of the developers. Thus, the accurate detection of malware has been a very essential step so as to protect our device from any infection or viruses. Malware is a kind of warning signal for your system and it also informs you are on a secure platform or not. Malware detection generally used an algorithm to calculate and analyse the numerical value that is unique to a specific virus. There are a few different types of malwares which are harmful and needs to be defended, they are spyware, trojan horses, worms, viruses and other forms of malicious code. Nowadays the malware detection and prevention technologies are widely available for servers, gateways, user workstation and mobile devices with some capabilities that offer tools to centrally monitor malware detection software installed on multiple devices or PC. In order to protect the data from malwares different kinds of artificial intelligence methods were used to recognise and classify malware such as Behaviour - based, Signature - based, API Call Attributes, Binary Attributes, Artificial intelligence approach etc. In the approach, same kind of technologies may be used to

identify more sophisticated malicious files. Additionally, it will be fascinating to evaluate the efficient efforts of other machine learning methods for the malware detection process.

Keywords: Cyber Security, Artificial Intelligence, Machine learning, Deep Learning, cyber-crimes, viruses, threats, IT Companies, Supervised Learning, Unsupervised Learning, Malware Detection, Signature – based and Anomaly – based Detection.

Introduction

The rise of cyber threats and the sophistication of malware in recent years have highlighted the need for advanced cybersecurity solutions. Artificial intelligence (AI) and machine learning (ML) have become powerful tools for improving cybersecurity, especially in the area of malware detection. This literature review provides an in-depth review of AI applications, machine learning algorithms, challenges, and future directions in the context of cybersecurity specifically designed for malware detection.

Artificial Intelligence or AI is a very huge branch in the IT sector. It is constantly developing and has human-like capabilities. There are numerous subsets of AI like Machine Learning (ML), Deep Learning (DL), Neural Networking, NLP etc. These concepts help in building machines which can mimic human behaviour and perform tasks which humans can perform. They can also help in building machines which have emotions and can feel things. These machines can constantly learn new things by themselves without any human intervention. Machine Learning or ML is a subset of Artificial Intelligence. It can be used to build a machine that can learn on its own. Machine Learning is in huge demand in today's world.

Deep Learning or DL is a subset of Machine Learning. It is a neural network which consists of three or more layers. These neural networks try to mimic the networks present in the human brain. AI helps the professionals to solve various problems. By using the latest methodologies, we can prevent a number of malicious activities taking place. By using machine learning, deep learning we can identify the data patterns of the company's security and different forms of cyber threats. AI or artificial intelligence in computer science is used for developing machines. It is a way of making computers or software which thinks and acts like humans. Cyber security consists of technologies and processes used to protect data, information from cyber-attacks. Nowadays AI in cyber security plays an important role. AI in cyber security is used for analysing and detecting risks from cyber-crimes which helps organizations to protect their important data or information. To protect data and information from cyber

criminals AI and machine learning is essential. Most of the cyber criminals use phishing attack techniques to hack data and information, to overcome such attacks AI is used.

AI and cyber security have a great future.

Reasons: -

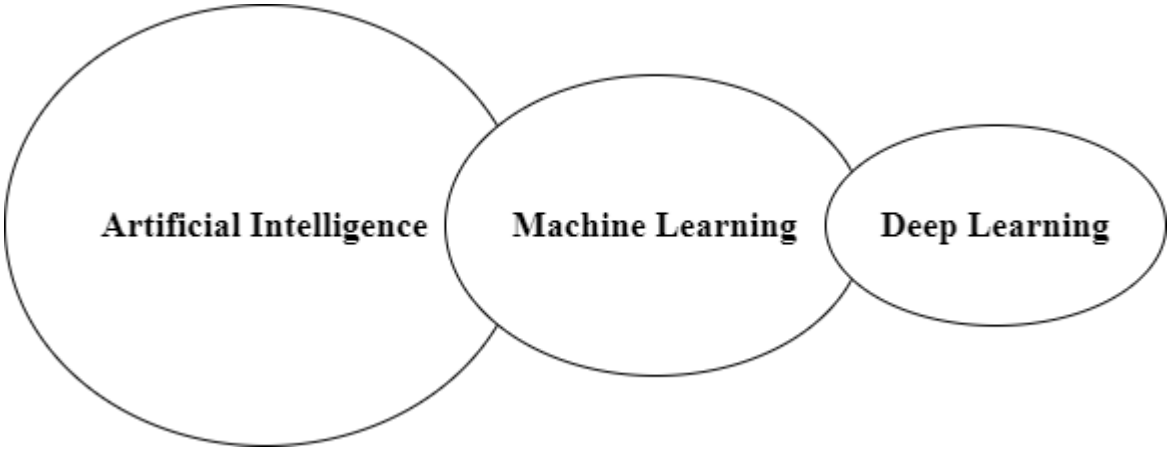
1. Used for security

2. Used to find threats in organization

3. Used for preventing attack

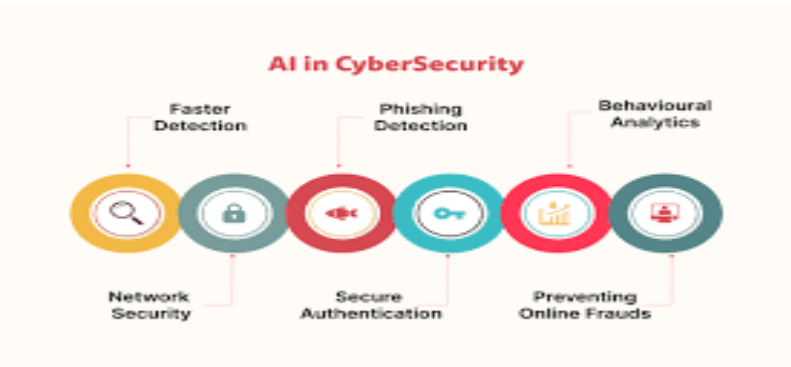
4. Used to improve network quality

Cyber security plays an important role for It companies and the government to protect their data.



1. Role of AI in Cybersecurity

1.1 AI's Put in Cybersecurity, Threat discovery and avoidance :-



Threat distinguishing proof and moderation is one of the most employments of AI in cybersecurity.

Large scale information investigation, design acknowledgment, and the discovery of anomalies that might demonstrate a cyber assault are all capabilities of AI calculations. Conventional rule-based frameworks can find it troublesome to reply to dangers that alter, whereas AI can overhaul its models powerfully depending on new information, advertising a more vigorous protection.

AI-powered danger discovery frameworks can keep an eye on client movement, endpoint action, and organize activity to spot conceivable dangers counting interesting framework utilization designs, whimsical information exchanges, or odd login behaviours. Early threat distinguishing proof and incite activity are made conceivable by this proactive strategy.

During an progressing emergency, AI-powered occurrence reaction frameworks may too allow real-time upgrades and bits of knowledge.

1.1.2 Enhanced Incident Response

In addition to identifying dangers, AI enhances event response by automating and accelerating the decision-making process. Based on accurate information and accepted best practices, AI may assess incident information, prioritize warnings, and suggest appropriate reactions. This shortens response times to incidents, reducing the potential damage brought on by cyberattacks.AI-powered incident response systems may also provide real-time updates and pieces of information during an ongoing attack, assisting cybersecurity teams in making informed decisions to contain the attack and prevent recurrences.

1.1.3 Vulnerability Management

AI can help in relating vulnerabilities within a system or network by bluffing implicit attacks and relating weak points. By prognosticating implicit entry points for bushwhackers, associations can proactively secure these areas and reduce the attack face. Machine literacy algorithms can help in automatically doctoring known vulnerabilities, minimizing the window of occasion for bushwhackers to exploit these sins.

2. Machine Learning

Machine learning algorithms are known for creating or developing patterns which can be manipulated with the use of different algorithms. It is used for pattern detection, face detection and cyber-crime mapping. Machine Learning has a prominent place in the industry of cyber security. Information security is benefited by machine learning due to its efficient tools used in various fields. There are numerous machine learning techniques which can enhance the correctness of threat detection and identify threats faster than humans. Cyber security systems, with the help of machine learning algorithms, can help to analyse various patterns which will help the system in turn to avoid cyber-attacks and adapt to changing behaviour. These techniques will also improve the network visibility and speed up the process of removing from cyber-attacks with the help of computational analysis. Several ML algorithms have made their way in the field of cyber security. It also helps to identify new and malicious software, improve fraud detection and secure user authentication. The most common applications of ML algorithms are spam detection, intrusion detection and malware analysis; they have a wide range of addresses in various ML problems. The present-day world has a boon for making human interaction proofs better, to evaluate protocol implementation, smart meter data profiling, and to develop authentication. Machine Learning algorithms can be classified into two types: supervised machine learning, unsupervised machine learning and reinforcement learning.

Machine learning techniques are beneficial for security in IT companies and the government. Machine learning is effective against threats and attacks.

Application of machine learning in cyber security

1. Identify cyber-attacks or threats

2. It Improve antivirus software

3. Used for fight against cybercrime using AI

1. Identify cyber-attacks or threats: -

The most important thing in cyber security is finding out requests for connections in the system. This application of machine learning has AI used for recording the history of calls and requests of connection in the system which is used for recording illegal activity.

2. Antivirus software: -

Antivirus software which is AI based is recommended everywhere for protecting our systems or devices from viruses by scanning all files in the system. This is done before using the system. Antivirus software becomes a

part of machine learning which tries to identify viruses and malware. Cylance software company builds an antivirus which is used to detect viruses and malware.

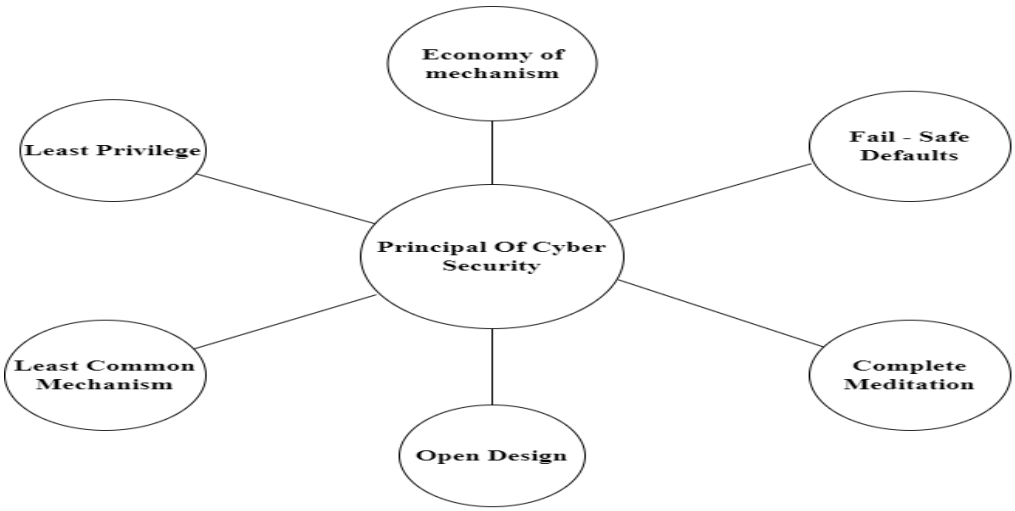
3. Fight against AI threat: -

Most cyber criminals take advantage of machine learning to hack the system or device. That's why it is very important in IT companies and government to fight against threats using machine learning

Machine learning algorithms identify and handle different types of cyber-attacks. Machine learning can be used by hackers to hack the captcha and password. Machine learning and AI nowadays become a Main reason to reduce risk of threat and attack. Phishing detection technique in machine learning used for identifying malicious URLs.

Today, as we enter in a technology driven world, cyber-attacks and threats have been increased on a large scale including immense data breaches, hacks into confidential data, and all digital platforms that the hackers can exploit. As a step to reduce these attacks, data engineers and cyber security experts are following the AI field to take part in using all the possible tools which included supervised and unsupervised learning techniques. The subset of Machine learning, popularly known as Supervised Machine Learning is known for its used of labelled datasets which helps in classifying data and predict outcomes accurately. As the risk of cyber threats are increasing, unsupervised learning methods may help to create Machine Learning Algorithms that can prevent cyber-attacks. Clustering, Representation Learning and Density estimation are some of the methods and processes known for unsupervised learning. These models will help to identify activities that seem suspicious, unknown or new, and alert the security team which will help to detect the malicious activities.

Principals of Cybersecurity: -



Economy of mechanism: -

Economy of mechanism states that the mechanisms that are used for security purposes must be short and simple. The designs and the implementation of mechanisms must simplify the whole process. Simple design and implementation will lead to lesser errors and the checking and testing will not be complicated. If the security framework is simple, it will be helpful for the developers and the users for better understanding and efficient development.

Fail-safe defaults: -

To understand this principle, we can go through a simple example – Suppose there is an operating system and we have a group for handling this system and we want to add new members in the group, the members of the default group will have lesser rights for files and services. So, this principle tells us that the system should be configured with a conservative protection strategy by default.

Complete meditation: -

Here’s an example – Suppose there an online website and the user has logged in after certain period say after twenty minutes the user should be asked again to log in as twenty minutes have elapsed.

So, the basic idea behind this principal is that every object's access must be verified to see whether it complies with a protection plan in order to determine whether it is permitted. The system should always verify the related access privileges whenever someone attempts to access an item.

Open design: -

According to this rule, the security of a mechanism shouldn't be dependent on how secretly it was created or put into action. It implies that security is not increased by complexity. This idea runs counter to the notion of "security via obscurity." This theory is applicable to many computers security-related procedures as well as information like passwords or cryptographic systems.

For instance, there is a DVD player and CSS (Content Scrambling System). The CSS is a cryptographic technique that guards against illegal copying of DVD movie discs.

Least common mechanism: -

This concept argues that the methods allowing resources to be shared by several users should be limited as much as feasible in systems having

multiple users. Because it restricts the distribution of resources, this approach could also be limiting.

Suppose, more than one person needs to access the same file or program, they should do so through distinct channels. This helps to avoid unintended effects that might result in security issues.

Least privilege: -

According to this rule, a user should only be granted the rights necessary to fulfil his duty. Not the user's identification, but the assignment of rights given to the user, is its main duty. This means that if your boss requests root access to a UNIX system you manage, you shouldn't grant it unless the person has a duty that calls for that degree of access.

Machine Literacy (ML) has surfaced as a vital tool in cybersecurity, empowering associations to enhance trouble discovery, anomaly discovery, and overall security posture. This literature review explores the operation of ML in colourful disciplines of cybersecurity, pressing the advancements, challenges, and unborn prospects. ML classifiers can be trained to categorize files or activities into either benign or malicious classes, aiding in the identification of malware.

Machine Learning (ML) offers several significant benefits when applied to cybersecurity, enhancing the overall effectiveness of threat detection, incident response, and security operations. Here are some key benefits of using Machine Learning in cybersecurity:

Automated Threat Detection: Quickly identifies potential threats.

Real-time Response: Enables swift responses to cyber threats.

Improved Accuracy: Reduces false alarms, improving accuracy.

Adaptability: Adjusts to new and evolving threats.

Behavioral Analysis: Detects anomalies in system behavior.

Threat Intelligence: Analyzes vast threat data for insights.

Malware Detection: Enhances detection of malicious software.

Cost-Efficiency: Reduces manual monitoring efforts.

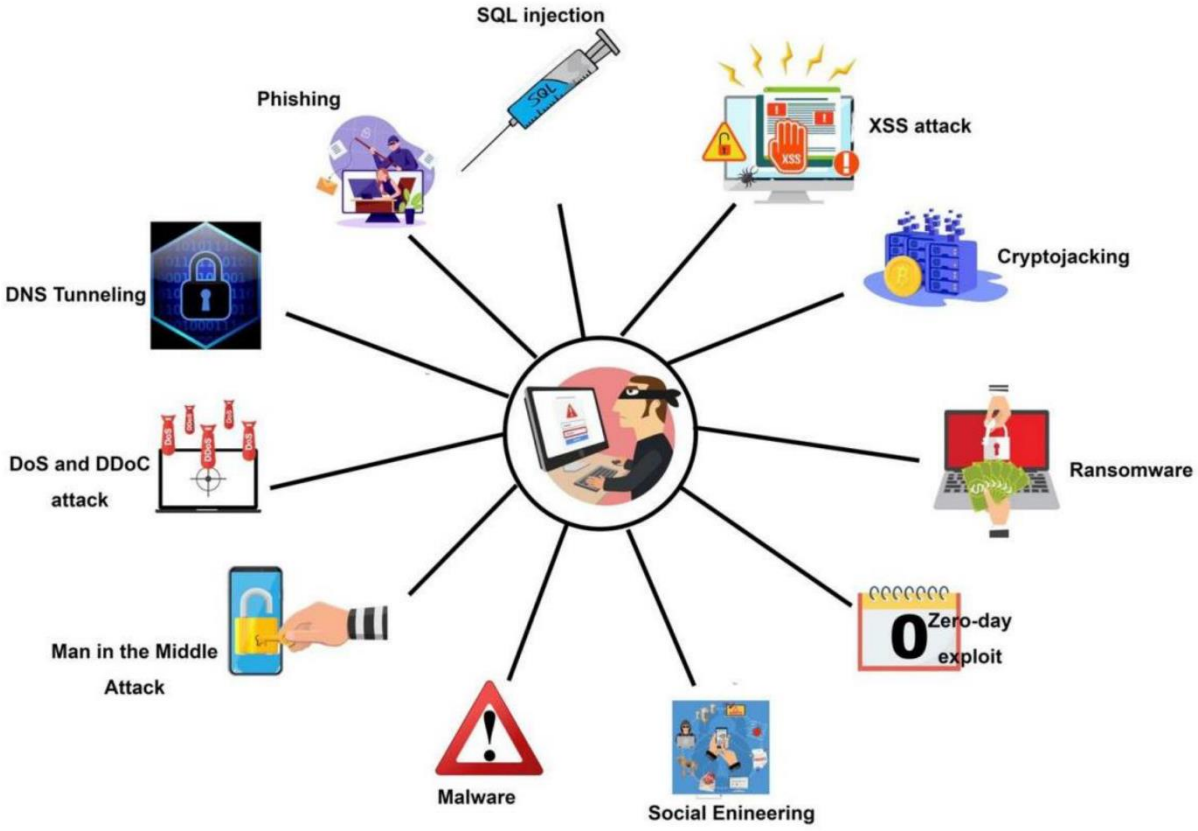
Optimized Resource Allocation: Prioritizes security efforts effectively.

Predictive Analysis: Foresees potential future threats.

UEBA: Analyzes user behavior for identifying threats.

Machine Learning in cybersecurity enhances detection, response, and protection against evolving cyber threats.

3. Malware detection



Modern cybersecurity relies heavily on artificial intelligence (AI), particularly when it comes to virus detection. It provides advanced tools to quickly evaluate large amounts of data in order to spot possible dangers. The following are the main methods AI is used in malware detection:

Pattern Recognition:

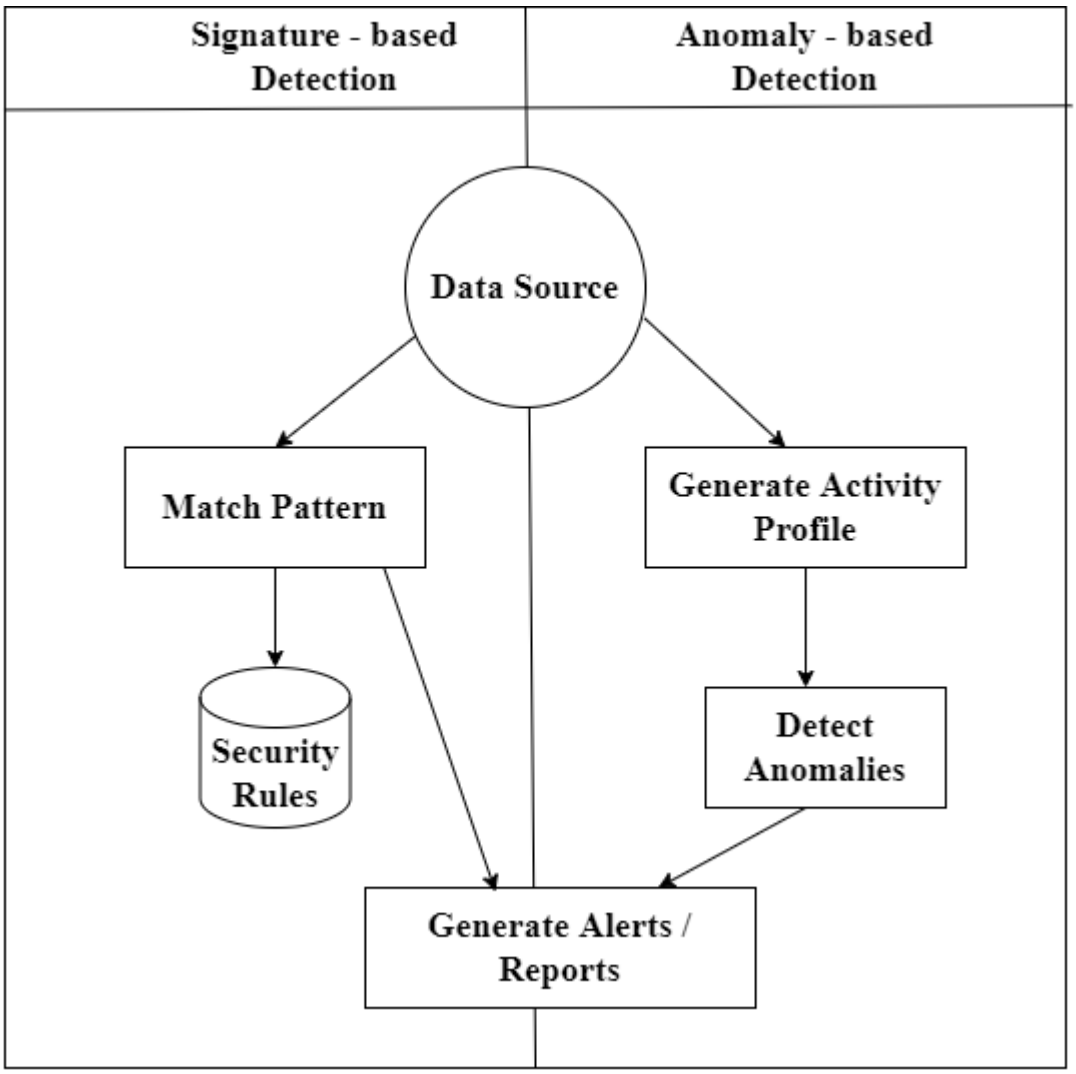
AI algorithms are particularly good at identifying malware-indicating patterns in files, network traffic, and system activity. This includes locating particular patterns, structures, or actions often connected to harmful software.

Anomaly Detection:

AI is able to create a baseline of typical system or network activity and identify any variations from this pattern as probable abnormalities. Unusual behaviour may be a symptom of malware intrusion.

Behavioural Analysis:

AI may carefully examine software or process activity to spot any suspicious behaviours like unauthorized access, data espionage, or efforts to change system settings.



Heuristic Analysis:

Using heuristics, AI can examine code and behavior to find suspicious characteristics that might be signs of malware. These heuristics are based on traits of known malware.

Detection of Zero-Day Threats:

AI may effectively find previously unknown or zero-day malware by studying existing malware and looking for comparable patterns in fresh, unidentified files or actions.

Signature-based Detection:

AI has the capacity to create and update malware signatures based on known malware samples, facilitating the quick identification and blocking of well-known malware strains. This is known as signature-based detection.

Deep Learning:

A subset of AI called deep learning models are skilled at examining the structure and content of files to find dangerous components. They can efficiently detect sophisticated and constantly changing malware types.

Network Traffic Analysis:

AI can use ensemble learning techniques to combine many detection algorithms, improving malware detection's overall accuracy and robustness.

AI is skilled in analyzing network traffic to find patterns linked to malware communication or command-and-control servers, which helps with early infection identification and prevention.

Phishing Detection:

Artificial intelligence (AI) can examine email content, URLs, and sender activity to spot phishing efforts, a typical method for spreading malware.

Botnet Detection:

AI can identify patterns in network traffic or user behavior that are suggestive of botnet activity, assisting in the early identification and mitigation of malware that is associated to botnets.

Utilizing AI for malware detection greatly improves the efficiency, effectiveness, and speed of recognizing and countering malware attacks, which is crucial in the changing world of cybersecurity.

Detection of Malware Technologies

Companies may utilize a variety of technologies, such as: to execute these strategies and efficiently identify malware.

Intrusion Detection System (IDS):

An IDS is a security tool that detects malware or other threats that are being installed on a system or that are entering a network. Security workers can analyze a warning that an IDS generates concerning the threat's presence.

Intrusion Prevention System (IPS):

An IPS is comparable to an IDS in that it protects the company against attacks more actively. The IPS not only detects threats but also prevents them from getting to the target system by sending an alarm.

Sandboxing:

Sandboxing is the process of dynamically analyzing malware in a secure, enclosed setting. Malware sandboxes contain a number of integrated tools for tracking the behavior of the malware, figuring out whether it is harmful, and outlining its capabilities.

Malware Analysis Tools:

To put the numerous malware detection methods previously mentioned into practice, malware analysis tools are readily available. For instance, static analysis often uses disassemblers like the Interactive Disassembler (IDA), but dynamic analysis typically uses a debugger.

Cloud-based infrastructure gives businesses the flexibility to improve their malware detection capabilities beyond what is practical on-site. IoCs may be distributed to users of a certain solution using cloud-based solutions, which can also analyze possible malware in sandboxes at scale.

Here are some intriguing AI applications in malware detection and defense that highlight their potential and influence:

Superhuman Detection Speed:

Millions of files may be scanned and analyzed by AI-powered malware detection in just a few seconds, but human analysts would need days or even weeks to do the same operation. In the quickly evolving cyber environment, this speed is essential.

Continuous Learning and Improvement:

AI algorithms continually enhance their detection skills by learning from every cyber threat they face. They get smarter and more capable of spotting novel and advanced malware strains as they analyse more data.

Detecting Polymorphic Malware:

To avoid being identified by conventional signature-based detection, polymorphic malware alters the look of its code. Despite these attempts at shape-shifting, AI can still identify the underlying dangerous tendencies, making it a powerful adversary for even the most cunning malware.

Changing with Zero-Day Threats:

Software faults known only to the vendor and users are known as zero-day vulnerabilities. Before updates are ready, AI algorithms can quickly identify and respond to assaults that take use of these vulnerabilities, offering a vital line of protection.

Natural Language Understanding for Deception Detection:

By comprehending the purpose and context of the language used, AI-powered natural language processing can evaluate fraudulent emails, phishing efforts, and social engineering assaults. This aids in safeguarding users by reporting questionable messages.

Cybersecurity professionals aggressively search for dangers within their systems using AI-driven threat hunting. A quick reaction is made possible by the AI's trawling through massive volumes of data to discover minute indications of potential breaches that may otherwise go undetected.

Synergy between humans and AI:

AI enhances human cybersecurity specialists by giving them cutting-edge tools for analysis and decision-making. The protection against cyber attacks becomes more efficient and effective as a result of this human-AI partnership.

Artificial intelligence (AI) can forecast potential future attack vectors by examining past attack data and seeing developing trends. Organizations may strengthen their defenses against impending dangers with the aid of this proactive strategy.

Real-time threat mitigation:

AI systems are capable of acting independently in response to threats, thwarting malicious activity and reducing harm. This quick reaction can considerably lessen the effects of an assault.

IoT Devices and Smart Systems Security:

As the Internet of Things (IoT) spreads, AI in cybersecurity is essential for protecting a huge variety of interconnected devices. AI is able to identify unusual behavior and security flaws in IoT devices, avoiding possible abuse by cybercriminals.

In addition to strengthening our digital defenses, the combination of AI with cybersecurity offers a safer and more secure online environment for people, businesses, and society at large. It's a fascinating, constantly developing field with a lot of potential.

For businesses, using AI and machine intelligence into cybersecurity has several advantages. Here are some details about how businesses might utilize AI in cybersecurity to identify malware and improve overall security:

Enhanced Threat Detection and Prevention:

Using AI-driven malware detection systems, businesses may identify complex threats that conventional antivirus software may have missed. For

the protection of key systems and sensitive data, this improved detection capabilities is essential.

Effective Resource Use: AI can automate and streamline the study of security logs, alerts, and incident reports, freeing security staff to concentrate their resources on looking into real risks. This effectiveness streamlines resource distribution and speeds up event response.

Cost-Effectiveness: While implementing AI-powered cybersecurity solutions initially may need investment, doing so often turns out to be economical in the long term. Saving time and money, AI can perform repeated activities and lessen the need for intensive physical involvement.

Scalability: AI-powered solutions are easily scalable to handle the complexity and number of cyber threats that are both increasing. AI's scalability makes sure that the cybersecurity infrastructure is efficient and capable of adapting to new problems as a business grows.

Customization and Adaptability: Machine learning models may be modified to meet the particular cybersecurity requirements of a business. AI can be tailored to offer the best security solutions, regardless of the sector, the type of data being secured, or the specific threat landscape.

Real-time threat information is provided by AI, which can continually monitor and evaluate the world's danger landscapes. For enterprises to keep ahead of new threats and proactively bolster their defenses, this intelligence is essential.

Reduced Response Time:

Automated responses powered by AI speed up the process of responding to cyber events. This short response time is essential for lessening the effects of a cyberattack and preventing serious harm to the company.

Long-Term Resilience:

Using AI in cybersecurity paves the way for long-term resistance to changing online dangers. Future-proofing an organization's security policy is possible thanks to machine learning algorithms that are able to continually learn about and respond to new threat vectors.

Regulatory Compliance:

Numerous regulatory frameworks demand that businesses have strong cybersecurity protections in place. By demonstrating a dedication to data security, using AI to improve cybersecurity not only aids in compliance with these rules but also offers a competitive edge.

Enhanced User Experience and Trust:

Businesses may increase user satisfaction and trust by successfully defending consumer data from online threats. Customers and clients have more security knowing that cutting-edge AI-driven security procedures are being used to handle and safeguard their sensitive information.

A company's cybersecurity strategy must now include AI and machine learning in order to remain ahead of cybercriminals in their game of cat and mouse. It not only improves security but also the organization's general effectiveness and competitiveness.

How AI in cybersecurity may help enterprises, with a particular focus on malware detection and preemptive threat mitigation

Advanced Threat Hunting: AI-powered systems may proactively search a network for dangers. These systems continually examine network traffic and data, looking for trends that might indicate malicious activity. With this proactive strategy, threats may be identified and contained early.

AI is capable of analyzing user behavior to find abnormalities that can point to insider threats. Artificial intelligence (AI) may detect unexpected actions like illegal access attempts or data exfiltration by analyzing the regular behavior patterns of staff and users.

Automation and orchestration of security measures: AI can automate reactions to specific security events, such as isolating impacted devices or blocking rogue IPs. On the basis of pre-established rules, this automation is organized.

Integration of threat intelligence:

Artificial intelligence (AI) is able to combine and evaluate threat information feeds from a variety of sources, combining and correlating this data to create a thorough picture of the threat landscape. This intelligence may subsequently be used by machine learning models to improve malware detection techniques.

Security Architecture That Adapts:

Organizations may implement a security architecture that adapts to the shifting threat landscape thanks to AI. Machine learning models are able to swiftly adapt to new threats and learn from them, allowing them to instantly modify security protocols and guidelines.

Detecting and preventing ransomware

AI is able to recognize the patterns and actions linked to ransomware attacks. A ransomware attack can be prevented or minimized by using machine

learning models that can identify file encryption procedures or anomalous file access patterns.

Enhancing the Security Incident Response Process:

Workflows for incident response can be automated with AI. This includes ranking situations according to their seriousness, recommending suitable replies, and even carrying out predetermined reaction procedures. These reaction tactics may be continuously improved by machine learning depending on the results of previous instances.

Vulnerability assessment that is ongoing:

Through analysis of settings, software versions, and other factors, AI can continually check an organization's infrastructure for vulnerabilities. In order to proactively patch or secure these vulnerabilities, businesses can use machine learning models to forecast probable sites of attack.

Classification of Malware Families:

Using data on malware's traits and behavior, AI can group the threats into distinct families. Security teams can develop specialized containment and cleanup techniques by using this categorization to better understand the malware's characteristics.

Detecting and preventing fraud

AI-powered solutions can be used to identify and stop fraud in online and financial transactions. Financial institutions and e-commerce platforms can take the necessary precautions to avoid financial losses when using machine learning models to identify trends linked with fraudulent conduct.

Organizations may dramatically improve their cybersecurity posture, keep ahead of developing threats, and create a safer digital environment for their operations, workers, and consumers by utilizing AI and machine learning in these ways. These tools enable security teams to quickly identify, address, and reduce online risks, eventually strengthening the organization's overall resilience.

Conclusion

Malware or malicious activities can cause a significant loss to all the sectors including finance, health and the confidential data in computer systems and Mobile applications. To ensure a good security for protecting all the data and hardware systems from malicious activities, AI, Machine Learning and Malware Detection comes into existence. Hence, having a detailed view of all the security measures, this study presents a detailed representation of the techniques and methods of malware detection using AI. The signature based methodology helps in detecting the malicious activities which matches the signatures present in the database. It helps in detecting only known virus. Then comes another technique named Anomaly based methodology which complements the limitation of signature method and provides a solution to detect unknown malware. This method makes use of a normalized baseline, which helps in detecting the malicious activity by detecting the change in the activity than that of the particular baseline.

A proactive and dynamic approach to cybersecurity is necessary given the increasing frequency and sophistication of cyberattacks. In the constantly changing IT ecosystem, artificial intelligence (AI) stands out as a powerful tool for bolstering security and staying one step ahead of dangerous actors.

References: -

- Binny Naik1, Ashir Mehta, Hiteshri Yagnik, Manan Shah, The impacts of artificial intelligence techniques in augmentation of cybersecurity: a comprehensive review, Complex & Intelligent Systems (2022).
- Nishita Gupta and Nilam Choudhary, Past to Future of Network Security with AI, Advances in Intelligent Systems and Computing, October 2020.
- Shidawa Baba Atiku, Achi Unimke Aaron, Goteng Kuwunidi Job, Fatima Shittu, Ismail Zahraddeen Yakubu, Survey on The Applications of Artificial Intelligence in Cyber Security, INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 9, ISSUE 10, OCTOBER 2020
- Sivasankar G. A., The Review of Artificial Intelligence in Cyber Security, International Journal for Research in Applied Science & Engineering Technology (IJRASET), 2022

- Md Jobair Hossain Faruk, Malware Detection and Prevention using Artificial, Intelligence Techniques,IEEE International conference on Big Data, Publisher IEEE(13 January 2022)