Sri Lanka Institute of Information Technology

Individual Project/Assignment

AI in Threat Detection within Cyber Security

Introduction to Cyber Security- IE2022

BSc Honors in Information Technology Specializing in Cyber Security

BSc (Hons) in Information Technology

Introduction to Cyber Security- IE2022

Year 2 Semester 1 - 2024

CASE STUDY NAME	AI in Threat Detection within Cyber Security
CAMPUS/CENTER	SLIIT KANDY UNI

Details of the Candidate

	Student Registration Number	**Student Name**
1	IT23222854	JAYASINGHE B. I

Contents

01. ABSTRACT 4

02. INTRODUCTION 5

What is AI in Cyber Security? 7

03. EVOLUTION OF THE TOPIC 7

3.1 Methods used in the past to secure the device. 8

3.2.1 Evolution of the Security 8

3.2.2 Using Artificial Intelligence to prevent threats from Social Engineering 10

3.2.3 Security Orchestration, Automation & Response Systems 13

3.3 Evolution of threat Alerts after Artificial Intelligence interference. 14

04. FUTURE DEVELOPMENTS IN AI IN THREAT DETECTION WITHIN CYBER SECURITY 16

05.CONCLUSION 17

06.REFERENCES 19

01. ABSTRACT

This research paper highlights how artificial intelligence quickly and efficiently analyzes data compared to humans improving Cybersecurity threat detection and programmed defense technology. In addition, this paper gives attention to how Artificial Intelligence protects the database, computer, network from attacks by predicting and detecting quickly.

Past methods used in cyber security are Network based intrusion defender systems and host-based intrusion defender and in this research, it contains how these security systems monitor network traffic in real time and tracking the user's routine and drawbacks in past security methods. Evolution of the ai detection in cyber security

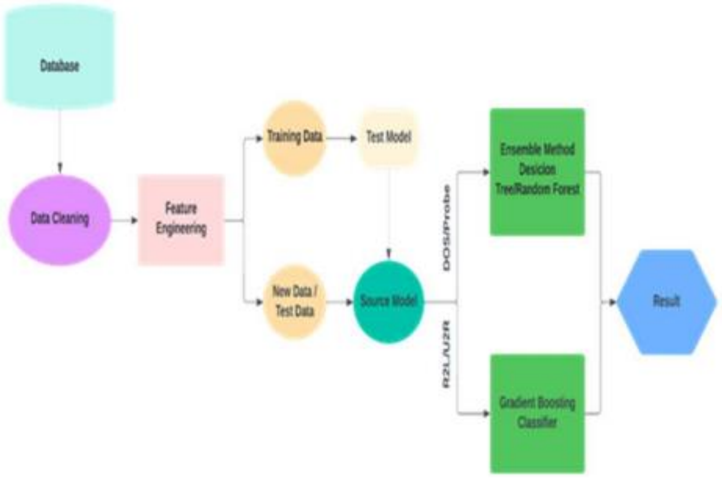
Moreover, this research paper contains the improvements of the Aritificial Intelligence adds to Intrusion Detection Systems. Intrusion Detection Systems helps the organization to monitor the network traffic if there is any suspicious behavior and it will automatically self-learn from the past cyber attacks which other organizations have faced in the past. Moreover, in this report it explores about the SOAR and how the AI in SOAR helps to improve accuracy of detecting threats and how it works and there is an automation to detect and response for phishing, vulnerability management and as well as the importance of it and future improvements of SOAR and security laws such as GDPR and HIPAA and real time threat mitigation without human involvement.

How the social engineering attacks work as well as how the attackers choose the victims. Attack strategies such as phishing, spear phishing, vishing or voice phishing, and baiting. Preventing methodologies that have been used by the Artificial intelligence and although artificial intelligence is active, we need user awareness regarding cyber threats so in this research those questions have been noted as well.

Although we have Aritificial intelligence we need an improvement in future as well as artificial intelligence helps in the present to mitigate the cyber threats and makes work easier to cyber security teams so all the technologies that have been mentioned above will be discussed in below.

02. INTRODUCTION

Rapid advancement of Information technology has greatly influenced how people, government as well as organizations interact with the networks. The universal use of cloud computing, large networks and linked devices has contributed to an extremely important depending on cyberspace for operational functions across various kinds of industries, including IT, healthcare and finance in addition to communication and data storage. Strong cybersecurity measures are required because of the major rise in the risk of cyber attacks that comes with robust cybersecurity measures.



Moreover, the field of cyber security is improving and getting advanced with the help of artificial intelligence and in the past era rule-based systems, manual monitoring, and signature-based defenses have been used to prevent threats. However, these previous strategies have found it difficult to mitigate with the evolving of cyberattacks, including ransomware, phishing, distributed denial-of-service or DDOS attacks, and data breaches. The research and use of Artificial Intelligence into cybersecurity frameworks has been caused by these challenges. Because of its capacity to handle vast amounts of data, identify patterns, as well as adjust to threat environments, artificial intelligence has become a powerful instrument that has the potential to completely transform cybersecurity. From this research paper elaborates on how Artificial Intelligence is being used as a game changer in the modern cybersecurity field. So, it explains the need for artificial intelligence is revolutionizing cybersecurity in the present day. It explains the importance of looking for real-time, evolving security mechanisms since standard techniques that heavily rely on human interaction and an unchanging rule set would not function. The primary advantage of Artificial Intelligence is the advanced data analysis it offers, particularly in machine learning and artificial intelligence, which improves systems' ability to identify potential risks by identifying errors from the usual patterns in network traffic, system behaviors, and user behaviors. In Artificial Intelligence in cybersecurity, the main role of machine learning is to detect threats. Large datasets with instances of known attacks and typical network behavior could be used to train models. These methods help to detect between harmful and a harmless activity with some degree of accuracy. From this method Artificial Intelligence helps to identify abnormalities in real time, frequently before human detects an attack. Random Forests and Support Vector Machines (SVM) are two extensively utilized machine learning algorithms. Random Forest techniques classify risks by generating several decision trees depending on the dataset's attributes. These trees are merged to produce the conclusion of whether the action is malicious or not. SVM, on the other hand, operates by finding the best limit between different types of data and it is very useful for malware identification and intrusion prevention Random Forests, Support Vector Machines, and a number of other machine learning algorithms have been used. Random Forest algorithms use a variety of decision trees based on collection attributes to categories threats. The final choice of whether the action is malicious is also produced by combining these trees. Finding the optimal border between the various data types is the basis for its operation. SVMs are especially effective in detecting malware and preventing intrusions, for instance, while SVMs can handle both malicious and authentic traffic. While traditional machine learning techniques are useful, more complicated threats involve advanced approaches. Convolutional neural networks neural networks and long short-term memory networks are two examples of deep learning models that are capable of processing even more complicated data structures than earlier techniques. Convolutional neural networks neural networks are primarily used for image recognition jobs, however by examining network traffic patterns, they can be modified for cybersecurity applications. Sequence-based learning is a strong suit for long short-term memory networks. This would make it highly successful in identifying APTs and zero-day exploits because they would be able to detect suspicious activity even in lengthy periods of network activity. As cyber threats develop AI's role in improving cybersecurity becomes more and more crucial. Because

AI has the ability to learn and adapt, it can automatically respond to even the most advanced threats. The worldwide AI demand for cybersecurity is rapidly expanding, reflecting increasing demand for AI-powered technology to defend key utilities, organizations, and individuals from constantly changing threats.

In addition, the development of Artificial Intelligence in cyber security field has become more dangerous in the present world. Help of the AI in cybersecurity has the ability to learn through previous threats it can learn through it analyze the attack and can prevent in future. So, because of that AI demand has risen due to defend utilizes that it benefits.

What is AI in Cyber Security?

Cyber Security is the way of preventing unauthorized individuals or harmful software or malware threat from being unintentionally infected to the users' devices and damaging their sensitive data or stealing their data. But when cyber attacks evolve and more upgraded the past era technology methods won't help to prevent as they are not enough to protect the devices. So due the technology advance we are in an era which has moved to Artificial Intelligence. Therefore, in the present we use Artificial Intelligence detection in Cyber Security, so it helps to detect and predict before a cyber-attack occurs and responds more effectively than monitoring it manually because Artificial Intelligence uses advanced computer technology.

03. EVOLUTION OF THE TOPIC

The field of cybersecurity has developed vastly, especially due to the evolution of AI and machine learning into security systems. Traditionally, rule-based systems. Traditionally, rule-based systems dominated the field of cybersecurity, relying on previously established signatures and threat detection and response rules. As cyberattacks grew more advanced and unexpected, these old systems became extremely inefficient. This section will highlight the evolution of cybersecurity from past methods to the powerful AI-enhanced system that currently exists, focusing on the major elements.

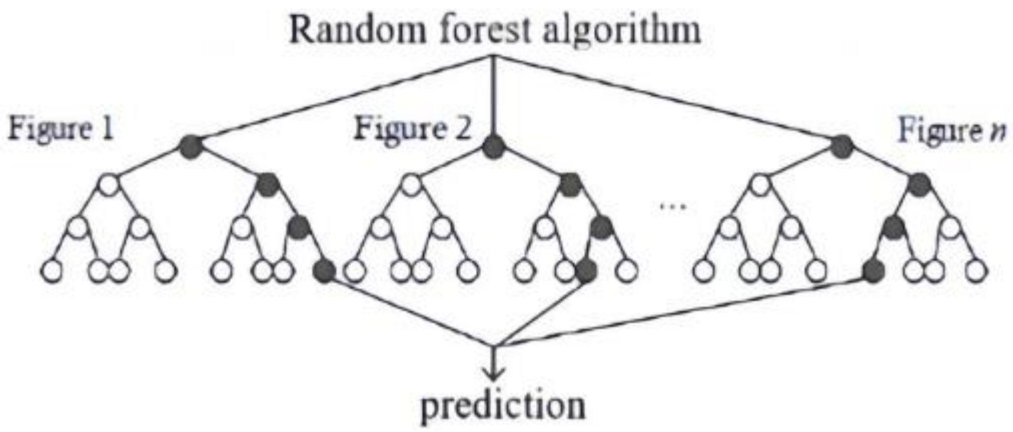
3.1 Methods used in the past to secure the device.

So therefore, in the past cyber security used the methods in traditional way such as by signature based and rule-based detection methods. So when considering the method Signature-based system can be introduce as it can detect the patterns or the way the malware or other malicious activities as if the system contain a virus in a the system database therefore the signature based system will scan the whole database which that type of same viruses contain in it ,although it detects the threat it can not perform as well to the evolving malicious threat as this method has limitations .

And the other method that has been used is Rule based systems. It detects that is there any behavioral activity or network traffic was malicious. And in this case, it can only detect manually as in this case its usual behavior is that it can only detect threats which have been previously discovered and this method will be useless against the zero-day assaults or unexpected, advanced ways of attacks. So, when the advanced of network system we need to have an advanced security system in the present.

3.2.1 Evolution of the Security

As the next step of the cybersecurity the anomaly based detection systems were created behalf of the improvement of the signature based system as this detection method monitor network traffic or it monitors the system activity against an overview of usual behaviours rather than in the previous stage it only detect the only the recognized threats .However, although it analyses it shows in instances in which harmless behavior was incorrectly classified as harmful although it is not a harmful behavior so this issue brought to an urgent solution to the users to which to be aware of both harmless and harmful behavior.so the vast evolution of the cyber security occurred after the combination of Artificial intelligence with cyber security. So, this evolution provided a way to overcome the drawbacks that happen in both signature based and anomaly-based systems limitations through machine learning. **[1]** Because this method is an automated detection which we had to use manual detections in previous systems so regarding the Artificial Intelligence system it can predict the future threats through understanding the previous knowledge of threats in the past which occurred this technology vastly help to detect cyber threats as it's a powerful comeback. So, after the knowledge of the previous threats machine learning reacts if an unusual behavior in real time without the assistance of a user. By the way in this scenario, there are not any limitations as it is learning from experience and improving accuracy over time. [1]



[1]

However, the most important use of Artificial Intelligence is concern into intrusion detection systems. Intrusion detection systems are made to monitor network traffic so it will in real time monitor if there is any unusual activity that may interfere with the system. As per the previous version of intrusion detection system was done according to certain signatures acknowledged the latest versions of all intrusion detection as it is combined with artificial intelligence exposed previously unknown attacks. And so far, now Artificial Intelligence helps to detect and respond to threats in real time. AI-enhanced security systems for intrusion detection use machine learning algorithms to analyze network data and identify advances that might be signs of the attack. This additionally involves looking for problems that show signs of malicious activity but don't necessarily correspond to any signature. For instance, even though an activity might not fall under one of these preset categories, it can detect as suspicious a sudden upturn in traffic coming from a specific IP address or an unexpected access to private information. As this detector learns from previous attacks that happened and predict any future attack and prevent. As the artificial intelligence in cyber security detect threat real time ,even though previous versions were detecting manually via a human interaction with system by monitoring every network and the database whether an attack is ongoing or infected as it is a slow error detecting security as well as it takes about several hours to fix the error or the threat but when considering that artificial intelligence can detect threats real time as well as it automatically initiating responses within seconds. Further in detail the advanced learning models such as Convolutional Neural Networks and Long Short-term Memory networks as well as these are also real time detection of cyber threats. [2] Convolutional Neural Networks are widely used to monitor network traffic behavioural even the smallest abnormality can be detected through it is a huge, advanced benefit for cyber security. Long Short-term Memory networks get to learn from real time data and recognize through it as frequently good for Advanced Persistent Threats which is known as long term anonymous attacks. In addition, there is another benefit which is through Artificial Intelligence that it can automate and detect attacks and as if the denial of service attack is detected for an instance it could begin the necessary precautions, such as rerouting traffic to avoid system overload or banning traffic from questionable IP addresses. This degree of automation is essential for avoiding harm, mostly in scenarios where maintaining service availability requires quickness. [2]

By the way Artificial Intelligence and cybersecurity continued to evolve as it evolves newer systems were more intelligent and also autonomous. Also using Artificial suspicious activities of the user as if a user using a new application rather than their normal routine Intelligence can detect any unusual network traffic as well as they good at detecting data access routine the artificial intelligence can easily trigger an alert to the system based on user behavior analytics even when there was no matching signature of such an attack.

3.2.2 Using Artificial Intelligence to prevent threats from Social Engineering

Social Engineering attacks are the most massive threats that the cyber teams face to defend against as they exploit human psychology as well as technological vulnerabilities. These attacks which was threaten by the cyber criminals manipulate users by exposing their sensitive or private information or performing actions that threaten security through phishing, spear phishing , vishing or voice phishing, and baiting are some types of common social engineering attacks used to aim and trick the users into steak their login credentials and even installing malicious software or transferring sensitive unwanted data to their devices and infecting viruses. [2]

So, in these types of cases, the growth of artificial intelligence in cybersecurity field has introduced new ways to prevent infection from social engineering attacks. While technological defenses such as firewalls and intrusion detection systems have evolved to protect the systems from such malware and network intrusions artificial intelligence has increased capabilities for detecting, preventing, and mitigating the risk of social engineering threats that target people's data in security. This is increasingly important because when social engineering threats become more advanced using social media to targeted messaging tricks to prey on victims.

In these sections we will explore how Artificial Intelligence technologies help to avoid social engineering threats and how the role of Artificial Intelligence response. As if a phishing attack was infected to a device by sending misleading emails by faking them as they are trustworthy entities in order to tricking them into clicking malicious links or providing sensitive information. That can be identified as Phishing. Likewise spear phishing is also described as a type of phishing that it disguise and adapt their messages as the victims get attract so it was specially create to the victims likes, the attacker collects data by monitoring the victims social media platforms. So when the evolving of security gets the attackers also improved their attacking strategies as they used emails and messages as well as using voice they have attack the victims which is voice phishing as they tried to act as trustworthy parties and tricking them by getting their personal credentials. Attackers construct a scenario the pretext to fool the victim, frequently copying a figure of authority, such as law enforcement or technical help, in order to get sensitive information. In this attack, hackers provide something such as free software or gifts to attract the victims into provide information or installing malware to their devices and infect their device secretly.

So, these types of strategies can not be captured by past versions of cyber security methods as well as the uneducated technology users doesn't know anything regarding these although rather than system vulnerabilities. However, the artificial

intelligence brings a huge impact to these types of weaken by monitoring real time for any unusual activities and it will automatically alert the users that no to download or it will restrict. So, when considering to the above-mentioned social engineering attacks artificial intelligence has trained to detect phishing attempts by predicting what would happen if we click any phishing emails more accurately than the signature based and rule-based detection methods. Artificial Intelligence system uses a new method which is Natural Language Processing. This analyzes all the emails message any other text-based communications we receive in real time. It evaluates the word choice, syntax and context as the Artificial Intelligence could detect if there is an unusual link which sometimes the phishing emails contain grammar issues or unusual language so through AI it detects and restrict those types of emails or messages which will alert the users device as need Immediate action or either the account will be suspend of the attacker. Further discussing machine learning models examine the email information as it's real time and user behavior to identify any unusual activities as if a user communicates using emails this methodology will be monitoring as if getting an email from an external source by requesting the victim's personal information and it will mark it then restrict the relevant sender. Although we use several applications in the device AI can learn the user's typical behavior overtime and it will spot the recent activities either the day-to-day applications done by the user and such as emails sent at unusual usage time or either from unidentified locations rather your own location and your device IP address. Google's Gmail filters and Microsoft's Office 365 are some advanced threat protections which are some social media that use AI powered anti phishing tools that are used to detect phishing emails.

Moreover, Real time fraud detection of is another area which artificial intelligence succeeds. Most of the social engineering attacks mostly focus on trying to hack financial systems by influencing the users to transfer payments or share financial details of the victims. Even though AI can't access the account fully it can monitor bank transactions if any unusual activity may occur through a social engineering attack. So, machine learning algorithms detect past transaction data to identify typical transaction patterns and alert any unusual activities and if occurs it will restrict it until it is verified. In many social engineering attempts, scammers pretend to be someone else to steal the victims sensitive information. AI-powered identity verification systems make use of biometrics, such as face recognition or voice recognition, to verify that the user who is accessing data is the relevant authorized user. This helps to keep attackers from prevent for stealing credentials or tricking users into providing information over the device or via email.

Security Awareness training is one of the most effective ways to prevent against social engineering. While technological solutions can prevent many dangers, users must be informed to identify social engineering strategies. AI improves security awareness training by providing individualized training modules based on employee risk profiles and behaviors.so when discussing about its phishing simulation Tools can help the user to mitigate threats while monitoring employee responses so based on that whether the user clicked an unusual link which is a phishing email or either avoiding it the system may deliver individualized training to enhance their ability to respond to these attacks. Over time, AI improves the training materials to target errors detected during testing.

3.2.3 Security Orchestration, Automation & Response Systems

Moreover, there is a security tool which was found by Gartner in 2015 which was named as "Security Orchestration, Automation and Response" SOAR these systems are to enhance cyber security which helps to organization to develop automated workflows by embedding Artificial intelligence with SOAR .Through this workflow system if the system got infected it will limit the threat of the infection and this will speed up and collaborate the process across different security systems. And, this process forwards the most critical issues will be forwarded to human monitoring on top of artificial intelligence operating on a SOAR process helps to improve the utilization of resources. So, this is a vast advantage to cyber security teams that they can concentrate on any other case. Splunk SOAR, Palo alto Cortex XSOAR, IBM Resilient, Swimlane, Siemplify

Security Orchestration - In this section refers to combination of several security tools and technologies. So, in this criterion it helps to work all the technologies smoothly as a SOAR system connects to a firewall, intrusion detection system and a threat intelligence system and it allows all the functionalities to share data, and it adapt to the relevant. [2]

Automation – In these criteria it is used to automate alerts, threat analysis and incident response without the interaction of a human being. Further discussing about it this process helps to restrict the Ips of relevant malicious websites. Automation can be an advantage to the cyber security teams because it automates data and any other malicious threat. So, in past versions they might provide false alerts but through this it will filter out false positives as well as low priority alerts to make it easier for cyber security teams. Moreover, common threats such as malware will trigger responses automatically by quarantining infected systems or it will automatically change the password without human intervention after that it will alert. [2]

Response – So although we had detection and alerts that will automate to threats, we need the most important technology which is quick response as in SOAR the RESPONSE technology helps to the cyber security teams to quickly mitigate to threats with this the ability to automate response by isolating corrupted or infected systems, executing firewall laws, or running a technical analysis. And helps to handle duplicate tasks at once and it mitigates the infection by it. This tracks and manages them and analyzes security incidents and response accurately. [2]

Automatically this system will detect phishing emails or any other attachments or links and then block the unauthorized irrelevant accounts acts as for phishing Response automation. Moreover, this can automate tasks for infected devices. This works as for an Endpoint Detection and response Integration threats. Vulnerability management can be done through this automatically through scanning for vulnerabilities infected patches and it monitors the network for unpatched systems. [2]

Aritificial Intelligence used to audit and verify the compliance with security standards such as The Health Insurance Portability and Accountability Act (HIPAA), General Data Protection Regulation (GDPR), The Payment Card Industry Data Security Standard (PCI DSS) such laws. AI systems may monitor for vulnerabilities, modifications to settings, and access control or the CIA triads concerns on a regular basis, AI may also be used to audit and verify compliance with security regulations like GDPR, HIPAA, and PCI DSS. AI systems may monitor for vulnerabilities, modifications to settings, and access control concerns on a regular basis, guaranteeing that enterprises are always in legal compliance. [1]

3.3 Evolution of threat Alerts after Artificial Intelligence interference.

Although in the past versions we had a secured detector in the past the system provides incorrectly detected legitimate behavior as malicious threats as well as sometimes these failed to detect an actual malicious threat. So, after the modern solutions for these issues, it has advanced anomaly detection methods to mitigate these errors. AI can more accurately recognize between harmless issues and real threats by continuously learning from practical instances and applying particular knowledge of the network environment. This capability enhances threat detection systems' accuracy.

Additionally, a system has been developed which is threat hunting. It involves an aggressive process of looking for online threats that have gotten around organizational systems security defense. By automating predictable procedures and recommending areas for further investigation, Artificial Intelligence can assist human analysts in danger hunting. Artificial Intelligence quickly analyses hundreds of millions of databases and network traffic data to identify suspicious behaviors that automated security systems might have detected. Then, cyber security teams can concentrate on identifying those anomalies, which enables them to focus concerns much more accurately.

It’s the ability of an Artificial Intelligence system to describe how it came to a specified conclusion is explainability. It has become more and more crucial in Cyber Security as the cyber security teams must trust the decisions which are made by the Artificial Intelligence systems. So, the cyber teams may better understand why a particular action was alerted as malicious which it helps in reducing false alerts and improves system trust. Such acts prove that artificial intelligence model isn’t a black box as its developing model which can be restrict a certain IP address which become a threat, and it will track down it. [1]

Although these AI models help to secure devices naturally this creates some conflicts regarding how personal data is gathered and processed when artificial intelligence monitors the vast amounts of network data. This would imply the guarantee that cyber security artificial intelligence achieves an ethical balance between user privacy and security. Cyber security is some sort of protecting the CIA triads which are Confidentiality, Integrity, Availability of a user although it is an artificial intelligence it should manage data protection laws, and the system takes responsibility for handling their personal data safely. Ethical issues also apply to decision making automation and it should be manipulated so as not to create unintended consequences by restricting unauthorized services and abnormal activities which are considered as threats.

04.FUTURE DEVELOPMENTS IN AI IN THREAT DETECTION WITHIN CYBER SECURITY

The future of Artificial Intelligence in Cyber Security is a completely autonomous security system. Which would lead to identifying an attack and AI will mitigate, fix security and repair vulnerabilities and even recovering damaged systems automatically without human or user interaction. So, the use of artificial intelligence to quantum safe security systems is an exceptional development in the cyber security field. With the production of quantum computing the current encryption protocols may become outdated. This encryption method will get developed with the power or the strategy of Artificial Intelligence and quantum technology that helps protecting sensitive data from future quantum-based decryption attacks. Through autonomous cybersecurity systems it has developed to self-learning from past threats that have occurred and through this automated detection it responses to cyber threats without human involvement as the automated detection is in real time. Self-healing capabilities, which means they will automatically fix vulnerabilities or restructure systems after an attack to provide future protection. [1]

Next method is predicting analytics to detect cyber attacks before getting infected to the device so that AI can predict upcoming threats by programming it's on through previous cyber attacks and through the network behaviors. Predicting model is a massive security model which helps to prevent any attack before such Advanced Persistent Attacks APTs and Zero-day vulnerabilities which are some challenging attacks that are difficult to detect through some normal security. As well as the role of SOAR in cyber security will be expanded as more organizations transition to artificial intelligence driven security. So, in the future we can ensure that these functionalities become more and more autonomous to identify vulnerabilities and to update their security patches or other updates on their own. And the predictive analytics will be vastly used by SOAR to avoid threats before getting infected which will evaluate and mitigate the need for physical interaction with the device. Enhanced AI integration will also ensure those responses optimized for the most recent threat environments. [1]

Using AI in future will automate the protection and patching of IoT devices that will help manage to ensure that the security threats that are in the devices are cured without human involvement. While current AI system technology mitigates and detect threat detection but, in the future, it will extend to where AI will manage the consequences of an attack that happened to your devices in addition to detect and prevent threats. Finding infected machines, removing them, and starting automatic recovery processes including patching, backup restoration, and configuration reconfiguration are all part of automated incident recovery. Finding infected machines, removing them, and starting automatic recovery processes including patching, backup restoration, and configuration reconfiguration are all part of automated incident recovery. Additionally, AI will investigate the fundamental reasons of events, offering analysis and suggestions for mitigating future attacks of this nature.AI will improve company efficiency by automating incident recovery, which will drastically cut downtime and data loss from an attack. [2]

05.CONCLUSION

The ability of AI to analyze a lot of data in real time, allowing for immediate danger detection and reaction, is one of its most important benefits. Response times to cyberattacks were delayed by the need for human involvement in traditional approaches. On the other hand, without human involvement, Artificial Intelligence includes systems are able to detect any suspicious behaviors, detect anomalies and even predict possible attacks based on previous threats that impact. The efficiency and speed of cybersecurity responses have significantly increased due to this real-time functionality, which also minimizes the area of vulnerability and mitigates the harm caused by attackers.

AI became a game-changing technology when previous cybersecurity techniques, such as rule-based systems and signature-based detection, was difficult to parallelly keep up with the evolution of the threats. AI has improved cybersecurity systems ability to identify and restrict the cyberthreats from malware and phishing to Advanced Persistent Threats (APTs) and zero-day vulnerabilities, by utilizing machine learning, deep learning, and natural language processing (NLP).

Future developments in AI for cybersecurity are exceptional and more convenient. AI will be able to identify and prevent and recover from cyberthreats without the need for human involvement once completely autonomous cybersecurity systems are developed. In addition to preventing attacks, these systems will fix themselves by detecting flaws and installing fixes on their own. Furthermore, AI's impact on predictive analytics will change cybersecurity from a reactive to a preventive strategy, enabling organizations to predict and avoid threats before they happen. The development of quantum-resistant security systems is another crucial field for future research. Current encryption techniques could become inaccurate as quantum computing develops, making data vulnerable to quantum computers' decoding. AI will play a key role in creating encryption algorithms that are secure against quantum attacks and enhance defenses against them in the future.

Finally, as concluding regarding the AI threat detection in cyber security has shown that this Aritificial technology is a game changer in cyber security field not only in cyber security to the whole world AI is a game changing technology. So, quantum-resistant encryption, autonomous systems, and predictive capabilities will improve security even further. In my point of view this technology will ensure the security of the devices and AI is one step ahead of attackers as the users can be ensure safety regarding their sensitive information.

06.REFERENCES

[1] Z. Xianni, H. Zhen, Z. Runfeng, P. Wang and H. Jia, “AI-Powered Cybersecurity: Enhancing Threat Detection and Defense in the Digital Age,” *AI-Powered Cybersecurity: Enhancing Threat Detection and Defense in the Digital Age,* p. 6, 2024.

[2] U. S. Rangrez, D. C. J. Kumar, S. A. Qadri and D. C. A. Kumar, “Cyber-Attack Defense System Enhanced by Artificial Intelligence,” *Cyber-Attack Defense System Enhanced by Artificial Intelligence ,* p. 5, 2024.