ASSIGNMENT

IT NUMBER: IT22345332

NAME: G.P DINUJAYA THAMARA

WEEKEND BATCH

MALABE CAMPUS

Table of Contents

Video Link

https://mysliit.sharepoint.com/:v:/s/ICS512/EfLm8Mg9zWhHvZrh0aGfczIBieiXs6kwKqILiGHNtWCjAA?email=amila.n%40sliit.lk&e=ofZvhf&nav=eyJyZWZlcnJhbEluZm8iOnsicmVmZXJyYWxBcHAiOiJTdHJlYW1XZWJBcHAiLCJyZWZlcnJhbFZpZXciOiJTaGFyZURpYWxvZyIsInJlZmVycmFsQXBwUGxhdGZvcm0iOiJXZWIiLCJyZWZlcnJhbE1vZGUiOiJ2aWV3In19

Abstract

In the present hyperconnected digital landscape, the endless and ever-evolving threat of cybersecurity-related threats looms larger than ever before. As the complexity sophistication and the content of these threats continue to escalate, the need for innovative and adaptive defense mechanisms becomes increasingly imperative. Artificial intelligence, a transformative and powerful force has reconceived the domain of cyber security. This report embarks on a multifaceted exploration of the role of Artificial Intelligence in consolidating our digital defenses. By mainly focusing on two key areas which are, Phishing Detection, and Malware Detection which offer an in-depth glimpse into the profound impact of AI on safeguarding the digital realm.

AI has emerged as a backbone in the domain of network security that advanced machine learning and Deep learning algorithms it empowers organizations to gain a profound understanding of network traffic patterns and another vital process conducted through AI is to identify anomalies that may signal cyber threats and foster real-time monitoring for proactive threat detections which is considered to be the core of cyber security domain.

Phishing remains a persistent and highly effective vector for cybercriminals due to enormous development of technology the Phishing attacks have become more and more complex and difficult to detect than ever before. This highly complicated and dynamically evolving AL possesses the capability to discern intricate patterns indicative of advanced deceptive practices and malevolent intentions.

In the relentless and continuously evolving landscape of cyber security malware represents one of the most persistent and adaptable threats. Cyber adversaries continually refine their techniques, developing malware that is not only complicated but also highly evasive. This continuous development of malicious software has challenged traditional cybersecurity approaches, demanding innovative solutions that can pace with the rapid mutations and polymorphic nature of modern malware. In this escalating arms race between cybersecurity professionals and cybercriminals Artificial Intelligence has emerged as a potent weapon against the threat of malware Deep learning models a subset of AI, has proven effective addressing in the challenges posed by polymorphic and evasive malware. The integration of deep learning models into malware systems has significantly enhanced our defenses against

the pervasive menace. These models excel in real-time analysis, swiftly categorizing and neutralizing threats, often before they can cause damage. Moreover, they reduce false positives, allowing security teams to focus their attention on genuine threats rather than benign software. By analyzing various factors deep learning can provide a multifaceted approach to malware detection. This multi-layered defense is crucial in today's threat landscape, where the variety and sophistication of malware strains continue to grow. In the pursuit of a more profound understanding of the intricate domain of malware, this report embarks on a rigorous exploration. The contemporary threat landscape is rife with an ever-growing spectrum of malware strains, each exhibiting diverse tactics, techniques, and evasion mechanisms. To effectively counter these dynamic and highly demanding challenges, it becomes paramount to delve into the depths of this intricate subject matter.

Another vital section of cybersecurity is security is Security log Analysis which is considered to treasure trove of information, but the enormous volume and the complexity of the data often overwhelm human capabilities. AI-driven analysis tools excel in processing vast volumes of data, identifying patterns and alerting security teams to potential threats.

Beyond these specified domains, I am conducting research into, The scope of AI in cybersecurity extends far and wide. It encompasses a broader vision that includes the integration of AI emerging technologies like IOT and blockchain. The integration of AL into the domain of cybersecurity is nothing short of a paradigm shift. It empowers us to confront the relentless and adaptive nature of cyber threats with confidence and resilience.

Introduction of AI in Cybersecurity

Before beginning consideration of the implementation of AI in the field of Cybersecurity, it is essential to establish a solid foundation understanding of AI itself. AI, often regarded as a milestone of modern technology, encompasses a diverse list of methodologies and principles that underpin its applications across various domains. This Foundational knowledge not only serves as a predecessor but also as an essential framework for comprehending the interesting role of AI in the context of cybersecurity.

In the domain of technology, Artificial Intelligence stands as a varied and continually evolving prototype. As per the consensus of numerous authoritative sources, AI can be defined as the emulation of human intelligence within machines, endowing them with the ability to process information, reason, learn from experience and adapt to new situations Over the years, AI has transcended conventional boundaries, evolving from elementary computer programs to systems of immense complexity.

Although AI has enjoyed a historical presence in computer programming, it is the convergence of advanced data structures, complex algorithms, and the dynamic fields of deep learning and machine learning that has ignited its transformative potential. This combination of cutting-edge technologies has catalyzed AI's capacity to replicate cognitive functions and decision-making processes with remarkable precision.

At present, AL's ability extends far beyond the confines of theoretical constructs, as it progressively finds application across diverse domains. This technological marvel exhibits the potential to transcend human capabilities in a multitude of fields. As we embark in this research, it becomes evident that AI's journey is self-possessed to redefine conventional standards, making greater and in certain instances, replacing human involvement in various fields of our present-day workforce.

AI is originated from 1956 when scientists and the researchers proves that machines could solve any problem if there enough resources for high performance computing in those days there was a program called General Problem Solver [1] In past AI is mainly focuses on robotics field and through the technological advanced researchers and scientist tried to automate certain processors therefore a need development the AI is vital through these AI is slowly and steadily developed in the present AI is used in every possible field. These development leads

to the developments of expert systems at first expert systems are not much complex as the human brain but they can be trained using different prompts and the data to get human solutions to real world problems.

The second milestone in AI was in 1965 through programs like Shakey the robot and ELIZA where conversations between humans and machines were automated. These early programs leads to development well known digital assistants like Siri, Alexa, Bixby and google assistant [1] After a decade without any invention the interest revolutionized this is because it was proved that machines were becoming better than human at simple tasks like playing checkers , chess and many more not only these there were an unnoticed development in the computer vision and speech recognition too to support the digital assistants. So these things paved the way to development systems that could understand and learn from real world with minimum human interactions [1]

In this vast domain of AI there two types of AI namely weak AI and strongly AI weak AI are limited to a certain task only but excellent in the designated tasks but the intelligence is very limited best examples is voice assistant on the other hand the strong AI are the system that human-level intelligence this category is capable of understanding , reasoning , learning and applying the previous knowledge to solve complicated problems these still in development process and well know train model in the present day is Chat- GPT which comes in different versions develop by open AI . Deep learning and Machine learning concepts are crucial when it comes to domain of AI because the whole AI is running because of advanced DL and ML concepts and algorithms. Deep learning DL is actually a subset of machine learning that is mainly used to train artificial neural networks and AI is learning through machine learning concepts [2]. From these machines learning techniques professional used AI to analyze networks detect anomalies and many more applications which were used in the domain of cyber security later the use of AI in cyber security developed further because of some key developments such as Behavioral Analysis, Predictive Analytics, Natural Language Processing and many more.

When we consider AI in network security analysis This is mainly impact on three areas Predictive Analysis, Automation and Threat Detection and prevention [5] and Network Analysis which is abbreviated as NTA is method which is used to monitor network availability and identification of anomalies detecting malware ,detecting vulnerable protocol and cipher usage, slow network troubleshooting are widely reported cases in the network traffic analysis

in the past this was done by the professionals name network engineers but now it has been slowly moving to AI because of the accuracy of deep learning and machine algorithms. The network analysis is a crucial role in cyber security because every device is connected through the network When we consider about phishing which is the most successful type of attack people are highly deceived by this attack especially non-technical people there are different types of phishing attacks the most common type is email-phishing [6] and other most common type of cyber threat is malware. Malware is simply named Malicious Software which is mainly used to attack a system. This is a piece of code that is very offensive in nature and can cause destruction and other unwanted effects to the systems. So oppositely malware detection is a set of defensive mechanism required block this legitimate attacking process there are different types of malware techniques widely use in threat analysis [8].

Evolution of phishing Detection and Malware detection

Phishing occurs on a distinctive methodology, one so complicated that even well-seasoned experts within the cybersecurity field can fall victim to its tactics. Its intricacies are designed with a level of shading that Transends the traditional cyber threats, making it a frightening challenge even for the most adept professionals in the domain. When we delve deeper into phishing techniques the basic element of this type of attack is simply a message which is sent through any platform. The complexity of phishing attacks amplifies in direct proportion to the number of features available in the platform. As the complexity of the platform increases these attacks are also progressively challenging to detect and mitigate. This escalating complexity necessitates heightened vigilance and advanced countermeasures from cybersecurity professionals to safeguard against evolving phishing threats. Normally the attacker uses public resources, especially social networks. Social networks are rich sources for cybercriminals to gather information about their target including their preferences, interests, and other personal details. Then the attacker can use this information to create a reliable fake message. If the attack goes to much depth it will lead to creating a fake profile. Through phishing attack, the attacker can get different information and can inject certain malicious codes and backdoors to the victim's machine. These attacks work because they pretend to be messages from sources the victim trusts, like the victim's boss, banks, or other well-known organizations. When these hackers pose as someone the victim relies on, it triggers the victim's natural trust in them. This tactic makes their phishing attempts seem more believable, making victims more likely to fall for their tricks. To protect, it's crucial to be aware of these sneaky tactics and stay vigilant against such deceptive schemes in the cybersecurity realm. In the past, spotting phishing emails was often possible due to their poor writing and the use of different fonts, fake logos, and layouts. These inconsistencies were telltale signs of a scam. However, as technology advanced, cybercriminals have become adept at crafting near-identical copies of genuine content. This increased sophistication in copywriting has made it much harder to detect phishing attacks. Now, the differences are often so subtle that even vigilant individuals can be easily deceived, emphasizing the need for advanced security measures in today's digital landscape.[7]

According to many sources, there are five main types of phishing attacks, Namely Email Phishing, Spear Phishing, Whaling, Smishing, and Vishing, Angler Phishing.

Email phishing is the most used attack, which is sent through an email. Attackers used fake domain names, and business logos and sent common requests emails, agreement type emails use a sense of urgency or a threat where the user suddenly takes action without checking the authenticity (for example our system has updated therefore, please enter the password in the following link). Fake domains usually replace characters that go unnoticed by the human eye (for example my-bank.com replaced by mybank.com) [7]. These phishing emails usually have a few goals bait links (causing the user to click to link to a malicious website, causing the user to download an infected file, and deceiving the user to provide personal data [7].

Spear phishing also uses email, but it is sent to a specific person. The attacker knows the overall details of the target Name, Job title, Email address are few of them. This level of detailed information enables cybercriminals to craft highly personalized and convincing phishing attempts, tailored specifically to the individual, thereby enhancing the deceptive nature of the attack.

In whaling it targets senior management and other highly privileged roles in these attacks the attackers don't use tricks like malicious URLs they send highly personalized messages on the information they have discovered so far[7].

In Smishing and Vishing, the attacker uses a phone. This is mainly done through verbally used social engineering techniques. The attacker always tries to use manipulative tactics to get the personal details of the victim. In this type attacker takes a different role (for example as a bank manager) Vishing also involves automated phone calls that ask the victim to type the personal details which is very hard to detect by human.[7]

Finally, Angler phishing is another method that uses fake social media accounts belonging to reputed individuals or companies for example attacker uses the same profile picture slightly changed email (abc-mobiles@gmail.com as abc—mobile@gmail.com) In this attacker takes the advantage of the customer's tendency to make complaints and assistance requests. When the victim requests some assistance the attacker directly asks for some personal details acting like the customer care of the company.

At present AI goes beyond signature-based detection, which hackers have learned to evade by tweaking some elements like HTML code or image metadata. Incorporating machine learning capabilities, AI focuses on detecting characteristics and behaviors related to phishing as opposed to known signatures [9]. AI can be used for both phishing attacks as well as phishing detection because Phishing attacks have become more complex than ever before Vishing attacks can be easily done because now it has AI voice technology which is a rapidly developing area in AI through this technology the Attacker can clone the voice which is pretty much identical to the original person through this the attacker can deceive the victim by creating an emergency situation where the victim gets confused and provide whatever the information asked. Since the attackers are using AI to advance the phishing attacks the security professional must also used to cope up with the required complexity of the attack in the present organizations automatically detect up to 99% of advanced phishing attacks through different AI-powered tools (for example AI AI-powered security email). [10] When it comes to the security domain These AI tools used use complex machine learning algorithms for phishing detection, they typically study behavioral pattern frequencies of the original voice communication patterns of the original voice and the individual, syntax [9].

The major drawback of AI models they totally depend on the data they are fed and the truthiness of those learned sometimes the attacker can inject malicious code edit data and create false data then whole phishing detection would provide incorrect results. Because according to many sources, the major blind spots of ML are fake datasets [9].

In the field of cybersecurity, malware assumes a pivotal role on the attacker's side functioning as a versatile tool capable of executing a wide array of malicious activities. It can be as a scripting program written using Python, a virus designed to infiltrate systems, or various other forms. Once the attacker successfully executes malicious code on a victim's computer, the attack stands poised for complete infiltration and control, thereby ensuring a high likelihood of success. As the threat landscape continuously evolves, so does the sophistication of malware. In response to these escalating challenges, the integration of Artificial Intelligence (AI) has revolutionized the process of malware detection. There are many AI algorithms, particularly those based on machine learning and deep learning which enable dynamic analysis of malware behavior, which allows real-time identification of patterns and anomalies this approach significantly enhances the detection capabilities.

A diverse array of malicious software, commonly referred to as malware, has proliferated in the modern technological landscape. These malicious entities come in various forms, each designed to exploit vulnerabilities and compromise digital security. The contemporary cybersecurity landscape identifies twelve prevalent types of malwares:

- **Ransomware**: software that uses encryption to disable a target's access to its data until a ransom is paid**.**
- **Fileless Malware**: A stealthy form of malware that operates within a computer's memory, leaving no trace on the file system.
- **Spyware**: As the name says spyware collects information about victims' activities without their consent
- **Adware:** Displays unwanted advertisements and redirects users to malicious websites.
- **Trojans:** Disguised as legitimate software, these can take control of victims' system.
- **Worms**: Self-replicating malware that spreads across networks, consuming bandwidth and compromising systems.IT typically slows down the victim's machine.
- **Virus:** virus is also a code but it runs if the infected program is running only mainly used to steal sensitive information difference between a Trojan and a virus is is Trojan can run without the infected program.
- **Rootkits/ Backdoors**: enable unauthorized access and control of the victim's computer. Malware that creates secret entry points into a system
- **Keyloggers**: Records keystrokes to capture sensitive information such as passwords and credit card details.
- **Bots**: Automated malware that performs tasks over the internet, often used in large-scale cyber-attacks.
- **Mobile Malware**: Targeting mobile devices, this malware compromises smartphones and tablets.
- **Wiper Malware**: Designed to erase data on a targeted system and designed to crash the system files.

Understanding the distinct characteristics of these malware types is crucial for cybersecurity professionals and users alike, enabling them to recognize potential threats and implement effective defense strategies against these malicious entities [11].

According to different sources, AI uses ten types of Malware Detection Techniques:

- **Signature Based Detection Techniques**: which is one of the oldest techniques in the present has become more complicated. This technique uses a known digital indicator of malware to identify suspicious behaviors. These lists of indicators are often maintained in a database [8].
- **Static file analysis:** In this method generally examines a file's code without executing the suspicious file to identify signs of malicious intent mainly examines file name, hashes, strings such as Ip address file header data can be determined whether a file is malicious or not [8].
- **Dynamic malware analysis**: in this method the suspicious file is malicious code is running in a safe environment called a sandbox. This is usually a closed system which help the related professionals to watch and study the actions of the malware [8].
- **File extensions blocklist/blocklisting:** File extensions are letters after the period attackers use this to deliver malware packages, so this is also a commonly used security method list known malicious file extension types in a blocklist to prevent the user from downloading those types of files [8].
- **Application allowlist/allowlisting:** This is the exact opposite of the blocklisting this authorizes to use certain applications which is on an approved list [8].
- **Malware honeypot/honeypot files:** honeypot usually describes software or an API to draw out malware attacks in a controlled, non-threatening environment. from this security teams can analyze the attack techniques and can redesigned a antimalware solutions [8].
- **Check summing/cyclic redundancy check (CRC):** This basically confirms the integrity of commonly used checksums is a CRC it analysis both value and position of a group of data. This is very effective to detect corrupted data [8].
- **File entropy/measuring changes of a files' data:** In this file's data the changed amount is measured through entropy can identify potential malware [8].
- **Machine learning behavioral analysis:** Machine learning which is sub section the AI through it learning capability through teaching algorithms through the existing data to predict answers on new data. This can analyze file behaviors, identify patterns, and use these insights to improve detection.[8]

Future developments

The fight against phishing assaults has reached a new phase in the field of cybersecurity. with outstanding technical developments. Modern tactics like Behavioral Analysis and URL Analysis have smoothly integrated with established defenses like Machine Learning Algorithms and Natural Language Processing (NLP). With the use of these advancements, we can now analyze phishing efforts' content as well as dig deeper and ascertain the true motivations behind these nefarious schemes. This level of comprehension guarantees a thorough defense against phishing efforts, more effectively securing our digital environments.

Technology advancements recently have shown a new area of security, presenting ideas like behavioral biometrics. This technology provides a further layer of security, enhancing how impenetrable our defenses are by recognizing small behavioral characteristics particular to each user. We are now more vigilant than ever against dangers that aren't only text-based thanks to the use of deep learning to image recognition. It gives us the ability to spot phishing efforts deftly concealed within visuals. Another cutting-edge technology is Cross-Platform Phishing Detection, which improves security across several platforms and makes it impossible for online threats to bypass security measures. In addition, Explainable AI (XAI), a fascinating technology, is integrated, providing transparency in the AI models' decision-making processes.

Firstly Explainable AI is simply a set processes and methods that allows human users to comprehend and trust the results and output created by machine learning algorithms. Explainable. Explainable AI is used to describe an Advanced AI model, its expected impact and potential biases this helps characterize model is best in building creditability and confidence when putting AI models in to production this also responsible for AI development. Humans may benefit from explainable AI by better comprehending and explaining machine learning (ML), deep learning, and neural networks. [12]

The difference between Explainable AI with normal AI is the decision-making techniques and methods they are using. In XAI the decision-making process can be identifies and explained but in the normal AI architect of the AI cannot fully understand how it does the work. XAI has various AI techniques Prediction accuracy, Traceability, Decision Understanding are a few of them mentioned [12].

Secondly using deep learning for image recognition in this field has three properties namely Image detection, image classification, and Image recognition with the Deep learning model it

uses several neural network architectures for image recognition. In general, these architectures are working like the human brain one commonly used one is Region-based convolutional Neural Networks or R-CNNs. This is mainly used for image recognition and object localization. In this technology the better the quality of training data, the more accurate and efficient the image recognition model is the most important parameter while training is size, quality quantity, Number of Color channels aspect ratios and image scaling are some of them. [13] Another widely used Model Family is YOLO which means you look only once this was first described in 2015 this approach involves a single neural network trained end to end that takes photography as input and predicts bounding boxes and class labels for each bounding box directly This technique offers lower predictive accuracy although operates at 45 frames per second and up to 155 frames per second for a speed -optimized version of the model.

Finally latest upcoming technology in phishing detection is Cross-platform Phishing detection which is more advanced and accurate than ever before this simply means detecting phishing attempts across multiple platforms gophish is a widely used open-source phishing framework that supports cross-platform Phishing detection.

So when it comes to malware detection we must pay much attention to malware detection developments as well because, through any type of attack, the attacker's main intention is to inject a malicious code into the victim's machine in this relentless battle against malware the security professional's tool kit has uplifted than ever before while Signature-Based Detection and Heuristic Analysis remain foundational with the emergence of new technologies such AI-Enhanced Sandbox Analysis, Zero-Day malware detection these security professional's will become strong than ever before

According to some sources, there has been some research on combining AI with sandbox one such project is the sandbox analyzer which was carried out by Bitdefender [14] simply put sandbox analyzer is built by in-house ML and behavioral heuristic models this is a powerful forensic tool used with Endpoint Detection and Response to enhance the defense mechanisms and security of a company this tools analyze suspicious files by applying certain payloads in-depth and they observe malware behavior by simulating real targets[14]. Another major development is the AI sandbox hub which was introduced by StoneFly. This is also an AI-based sandbox appliance that has unique features like users to train the AI model per their specific

requirements. This has enhanced Data Privacy and Security and is also another important part is its availability. [15]

Another important turning point of AI in cybersecurity is zero-day malware detection in general zero-day malware is a considerable threat since it exploits unknown and unprotected vulnerabilities typically there are detection systems are two types namely signature-based detection and anomaly-based detection systems. For zero-day attacks, since they are new vulnerabilities anomaly-based detections are used. For this Machine learning has been great support because it's algorithms are built based on sample data known as training data. Sim[ply put these processes the data and deriving the feature vector, through an n-dimensional vector of numerical features that captures the characteristics of attacks, is challenging. The design of feature vectors often requires the domain knowledge of cybersecurity practitioners and is especially important in designing a zero-day attack ML mode. The existing zero-day attack detection studies show that data used in both training and testing are limited, therefore evaluation results fail but with new technology, this may be much more than ever before [16].

Conclusion

The threats present in cyber-attacks are greater than ever in today's hyperconnected digital world, where the cybersecurity domain is continuously changing. These dangers are becoming more complicated and evolving. We must use cutting-edge and flexible defense methods to protect ourselves from these always-changing dangers. In this comprehensive investigation, we've probed the significant contribution artificial intelligence (AI) makes to elevate our digital defenses, focusing on two crucial areas which are phishing detection and malware detection.

The Emergence of AI is a milestone in this digital world mainly in the field of network security which is supplemented by advanced machine learning and deep learning algorithms. This empowers companies and interested parties to gain valuable information about network traffic patterns and identify anomalies that may signal cyber threats. Real-time monitoring which is driven by AI has become a turning point in modern cybersecurity forming the bedrock upon which our digital defenses are built.

Phishing, a persistent and highly effective vector for cybercriminals, has evolved into a more advanced and exclusive threat than ever before. The continuous development of technology has given rise to more intricate phishing attacks, making traditional detection methods less effective. However, AI with its remarkable capabilities, has stepped up to the challenge Through the discernment of complicated patterns indicative of advanced deceptive practices and evil intentions Because not only the attacker side but also the defense side is also upgraded and the ability to detect the deceiving messages have relatively easy than ever before. The future is phishing detection looks promising, with advancements such as Behavioral Biometrics, Deep learning for image recognition, and cross-platform Phishing Detection. Behavioral biometrics adds an additional layer of security by identifying subtle behavior patterns unique to each user. On the other hand, Deep learning for image recognition extends our attention beyond text-based dangers. This enables the detection of phishing attempts used with replicated logos and through the cross-platform Phishing Detection phishing attempts across various platforms are uniformly detected, providing comprehensive security coverage. At last Explainable AI (XAI) might be the most powerful technological development that is being developed. Is shedding light on the decision-making processes of AI models, Enhancing trust and confidence in phishing detection.

Malware, an evolving threat, continually threatens cyber security professionals with it multi-formed nature. This amazing technology through deep learning models has revolutionized

malware detection. These models are excellent in real-time analysis, swiftly categorizing and neutralizing threats before they can cause damage. They significantly reduce false positives, enabling security teams to confidently focus on genuine threats The integration of AI-enhanced sandbox analysis, zero-day malware detection, exfiltration pattern recognition, and the innovative use of blockchain for secure data sharing has directed to a new era of defense. with the latest upcoming technologies such as AI sandbox analysis and zero-day malware detection anticipates previously unknown threats, staying one step ahead of adversaries Exfiltration pattern recognition allows one to identify exfiltration attempts more easily than ever before while blockchain technology fosters secure collaboration between cybersecurity entities.

However AI in cybersecurity is clearly by its continual innovation and an ever-evolving field of technology when AI is evolving it definitely promises more complicated solutions to modern cybersecurity threats and this bridges the gap between human intuition and automated detection which somehow reduces the workforce of people

In this report, I have explored AI's crucial role in shaping the future of cyber security. AI stands not only as a technological marvel but as a confident tool in battling against endlessly evolving cyber threats. Its ability to emulate and simulate human intelligence, process vast amounts of data, and adapt to new situations positions it as the cornerstone of digital defense. In this ever-evolving landscape, the combination of human expertise with AI-driven innovations becomes uppermost The collaboration of human intuition and machine learning algorithms creates a symbiotic relationship where each strengthens the other.

References

1. https://www.red-gate.com/simple-talk/development/data-science-development/introduction-to-artificial- intelligence/
2. https://www.simplilearn.com/tutorials/artificial-intelligence-tutorial/what-is-artificial-intelligence
3.https://www.geeksforgeeks.org/artificial-intelligence-an-introduction/
4.https://books.google.lk/books?hl=en&lr=&id=HACaS635bYcC&oi=fnd&pg=PA1&dq=introduction+of+AI&ots=Km8ztX2P0N&sig=HmXx-k_vAFWIiloMdEjbklJNuVA&redir_esc=y#v=onepage&q=introduction%20of%20AI&f=false
5. https://www.linkedin.com/pulse/securing-networks-artificial-intelligence-impact-ai-network-pathak/
6. https://www.rapid7.com/fundamentals/network-traffic-analysis/
7. What is Phishing? Types of Phishing Attacks- Check Point Software
8. Malware Detection: 10 Techniques- CrowdStrike
9. AI Goes Phishing (analyticsindiamag.com)
10. How AI is Fueling the Evolution of Phishing Attacks (ironscales.com)
11.12 Types of Malware + Examples That You Should Know (crowdstrike.com)
12. What is explainable AI? | IBM
13. https://machinelearningmastery.com/object-recognition-with-deep-learning/
14. Sandbox Analyzer- Bitdefender GravityZone
15. StoneFly Introduces AI SandboxHub™- AI-Based Sandbox Appliance
16. A review of Machine Learning-based zero-day attack detection: Challenges and future directions- ScienceDirect