UNIT 3 USE CASES FOR AI IN CYBER SECURITY

3.1 THREAT DETECTION

3.2 IMPROVING AUTHENTICATION

3.3 FASTER THREAT RESPONSE

3.4 SOCIAL ENGINEERING DETECTION

3.5 VULNERABILITY ASSESSMENT

3.6 USER BEHAVIOUR MODELLING

3.7 USING ML AGAINST SMS SCAMS

3.8 AI-BASED ANTIVIRUS SOFTWARE

3.9 EMAIL MONITORING

3.10 FIGHTING THREATS WITH AI IN CYBER SECURITY

3.11 USING ML FOR SECURING MOBILE ENDPOINTS

3.12 EXAMPLES OF MACHINE LEARNING IN CYBERSECURITY

- 3.12.1 SPEAR PHISHING
- 3.12.2 WATERING HOLE
- 3.12.3 WEBSHELL
- 3.12.4 RANSOMWARE
- 3.12.5 REMOTE EXPLOITATION
- 3.12.6 DENIAL OF SERVICE ATTACK
- 3.12.7 DNS POISONING
- 3.12.8 PORT SCANNING

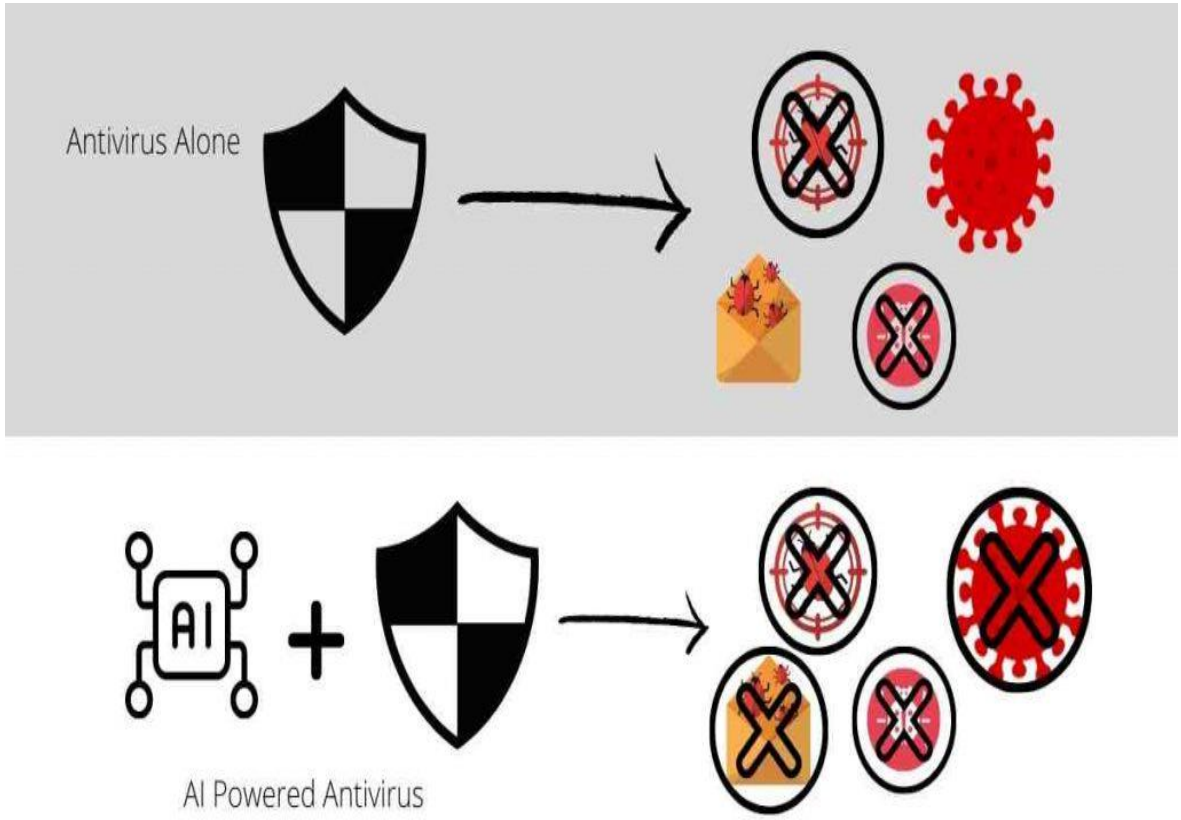
INTRODUCTION

- Cyber security is a major challenge in modern business operations
- Artificial intelligence has the potential to significantly improve the war on cybercrime. It can be used to reinforce cybersecurity best practices and minimize cyber threats through real-time monitoring and early detection of attacks.
- In addition, AI can be trained to understand cybersecurity threats well and provide protection against more advanced threats.
- The number of use cases for AI in cybersecurity is growing.
- AI capabilities like machine learning, deep learning, and natural language processing can complement security professionals' work to increase cybersecurity effectiveness.
- Understanding where AI provides value can help company leaders determine how to deploy it against phishing, zero-day exploits, and more.

1. THREAT DETECTION

- Essentially, antiviruses scan files for known malware signatures and quarantine files that turn out positive.
- **The challenge with this mechanism is that antiviruses have to be updated regularly to keep up with malware upgrades to provide ultimate protection**.
- One of the most significant artificial intelligence applications in cybersecurity is advanced threat detection. Unlike traditional signature-based threat detection systems, AI-based threat detection involves the observation of abnormal behaviour.
- **Use Case: AI-Powered Intrusion Detection**
- **Problem:** An organization wants to protect its network and systems from cyber threats, including unauthorized access, malware, and other security breaches.
- **Traditional intrusion detection systems (IDS) generate numerous alerts, many of which are false positives, overwhelming security teams and leading to a high number of missed threats.**

SOLUTION: IMPLEMENT AN AI-POWERED INTRUSION DETECTION SYSTEM THAT USES MACHINE LEARNING ALGORITHMS TO IMPROVE THREAT DETECTION ACCURACY AND REDUCE THE NUMBER OF FALSE POSITIVES.



- AI enables security software to think like a hacker and thus detect vulnerabilities that cybercriminals would normally exploit. In addition, it can detect weaknesses in your devices and alert you before a threat has occurred so you can take precautionary measures.
- **When paired with a traditional threat detection system, you increase the probability of detecting more threats with great accuracy**.
- Also include one of the most effective applications of artificial intelligence techniques - a robust VPN service like ExpressVPN to add an extra layer of security.

USE CASE

- A US-based healthcare service provider deployed an AI-powered threat detection system to augment its existing antivirus. The new system immediately detected and blocked 3 custom-designed malware that the traditional antivirus wouldn't identify.
- The company also realized a lower performance impact of each endpoint and increased monetary benefit for consolidating their antivirus solution

ENVIRONMENT • 400 locations • 10,000 endpoints • 1.3 million patients

CHALLENGES Reduce the number and severity of malware outbreaks

Prevent theft of personally identifiable information

Protect sensitive research and development information

Assess vulnerabilities in medical devices produced by the company

Safeguard 1.3 million patient records and comply with HIPAA regulations

SOLUTIONS Deploy CylancePROTECT® to 10,000 endpoints

Compromise Assessment service to identify if a breach occurred

Penetration Test of medical devices and supporting infrastructure

AI CYBER THREAT SOLUTIONS

- **Automation and False Positives**
- Security Automation, which identifies potential cyber-security incidents by monitoring abnormal data use, is key in defending against cyber threats.
- AI and machine learning are powerful tools in the field of security automation and can evolve the monitoring, prioritization, and alert processes to the next generation to cut human labor costs and speed up threat management cycle time.
- Humans remain in the loop only for the purpose of identifying false positives.

AI CYBER THREAT SOLUTIONS

- **Predictive Analytics**
- With emerging technologies becoming more and more involved in cyber attacks, simply gathering data or creating digital signatures is no longer sufficient for fast threat detection.
- Introducing AI solutions allows the system to monitor a wider number of factors and better identify patterns of abnormal activity. By leveraging this data, AI and Machine learning can be trained to track information and deliver predictive analysis.
- For example, suppose we know that there's a high risk that a certain type of virus will be released on Tuesday. In that case, a predictive analytics model will make a forecast about whether Tuesday is a good day to release a virus to try to catch the virus before it gets released.
- Example: Markov Chain Monte Carlo (MCMC) is a statistical method that estimates the probability of a future event given the probability of another event.
- It does this by running multiple future simulations to make the best guess for what will happen.
- It can handle missing data, making it a good fit for cybersecurity, where data might not be entirely accurate.
- Hyper-Parameter Optimization can help organizations optimize parameters based on data. The goal is to make predictions as accurate as possible while also making predictions that are more likely to be correct.
- Sensitivity analysis determines how much an event will affect overall business revenue. It involves calculating the expected revenue and potential revenue losses due to an event and comparing these values to a business's risk tolerance.

AI SOLUTIONS IN REAL USE CASES
CASE STUDY: MIT AI2 SYSTEM

- MIT's AI2 System is able to work through raw data and leverage unsupervised machine-learning algorithms to detect abnormal information security activities.
- The system is composed of Artificial Intelligence and Analyst Intuition (AI) components, for this reason, it was named by the experts Artificial Intelligence Squared (AI2).
- The system summarizes patterns and provides detailed information to security operators for further decision-making.
- The decision records act as auto feedback to the core machine-learning model to improve its algorithm for future analysis.
- The AI2 system's AI-human fusion achieved an impressive cyber attack identification rate of nearly 86%.
- Reference: https://youtu.be/b6Hf1O_vpwQ

AI SOLUTIONS IN REAL USE CASES
CASE STUDY: STARTUP SCENE

- *Sentinel — Home Security*
  The home security company Deep Sentinel leverages deep learning algorithms for property-related safety concerns. The product combines algorithms and computer vision technologies to quickly analyze threat factors in raw video stream data.
- Sentinel uses advanced, built-in artificial intelligence to assist cyber security analysts in analyzing data collected across an organization's network infrastructure, both internally and externally.
- Sentinel has been designed to collate data from virtually every source that an organization uses. This includes a huge variety of applications (mobile and web), servers, users, and devices, whether they are based on-premises or on the cloud.
- The company is also researching the use of autonomous drones and IoT devices in environmental data collection for security solutions. Deep Sentinel's products aim to leverage pre-trained systems to build a comprehensive home control platform.

- *Cloudflare — IoT Security*
- Cloudflare released its Orbit IoT security solution in 2017. Obert is an IoT security solution that enables IoT device manufacturers to connect their products to Cloudflare's network automatically, providing users with a machine-learning-based API to monitor suspicious activities.
- Cloudflare Orbit solves problems at the network level by creating a secure and authenticated connection between an IoT device and its origin server.
- Cloudflare provides an extra layer of security that allows us to keep our devices continually updated and ahead of any vulnerabilities.
- The combination of NVIDIA accelerated computing technology and Cloudflare's edge network will create a massive platform on which developers can deploy applications that use pre-trained or custom machine learning models in seconds.

USE CASES OF AI AND ML IN CYBERSECURITY

- **#1. Network Threat Identification –**
- Maintaining the network's security of business includes identifying the connection requests that are legitimate and attempting an abnormal connection behavior like receiving and sending large amounts of data or having exceptional programs after the connection to the enterprise network.
- An AI-powered network security system will monitor all outgoing and incoming calls to detect any suspicious patterns in traffic information. The data in question is generally high for human cybersecurity professionals to accurately classify threats.
- **Example:**
- Versive, the AI vendor provides AI-based cybersecurity software that uses dissonant detection to detect vulnerable security threats. The organization says its software helps banks and financial institutions to detect adversary identification and security threats.
- Versive offers Versive Security Engine, a solution that empowers security teams to automate advanced persistent threat detection, insider threat detection, malicious domain identification, data exfiltration early warning, and regulatory compliance aspects.
- Now owned by eSentire, Versive will offer enterprise Cybersecurity named 'VSE Versive Security Engine', that helps the financial and banking sector analyze all the transactions and secure related data using ML.
- Versive banks refer to the proxy, DNS, and Netflow as inputs to the Versive security engine. This software can monitor networks by using anomaly detection software in order to alert human authorities in case of discrepancies in data similar to events in previous cyber threats.

- **#2. AI-based Antivirus Software –**
- Antivirus software can work by scanning files on the company network to check whether any of the file matches the signature of viruses or known malware. The issue with this methodology is that it is reliant on security upgrades for the traditional antivirus software when new viruses are found.
- Conversely, AI-powered antivirus software mostly uses anomaly detection to monitor program behavior. Antivirus systems that use AI focus on identifying abnormal behavior generated by programs rather than syncing known malware signatures.
- This type of software works well for previously encountered, and recognized threats by its public signature, and new threats will not be detected and resolved easily by this traditional antivirus.
- **Example:**
  Cylance, a software company claimed their smart antivirus product offers AI technology to detect, respond, and predict threats.
- Unlike traditional antivirus software, Cylance's AI-adopted smart antivirus does not require virus signature updates, but over time it will be learning to detect malicious programs from scratch to end.

- **#3. User Behavior Modeling –**
- You know? Some kind of security attacks on business systems can motivate particular user in the company by knowing their privacy login credentials without their insight.
- Cyberattackers who have taken a client's accreditations can access to company network through in fact genuine methods and are very difficult to stop and detect.
- Thus, AI-based risk management systems can be utilized to identify changes in those methods and to determine password patterns of explicit customer behavior. In doing so, they will alert their Cybersecurity teams when the pattern does not work.
- **Example:**
- A pioneer AI vendor called 'Darktrace' has provided Cybersecurity software, which they utilize as ML to analyze network traffic information in order to understand the baseline behavior of each user and device in the firm.
- Taking inputs and other training datasets from subject matter experts, the AI-software learns to detect a vital deviation from normal baseline user behavior and instantly alerts the company to cyber threats.

- **#4. Fighting AI Threats –**
- Since hackers are now using AI to detect points entering enterprise networks, organizations should increase the speed at which they can easily detect Cybersecurity. Therefore, the use of AI software to protect against AI-adopted hacking may become an essential part of security defense protocols in the coming years.
- In the past few years, firms across the globe have submitted to ransomware and cyberthreats attacks such as Notepetya and WannaCry. These kinds of cyber attacks will spread fast and affect a large number of computers. Those who carry out this type of attack are more likely to use AI technology in the future. The benefit that Artificial Intelligence can give these hackers is similar to what AI provides in companies: faster scalability.
- **Example:**
  Cybersecurity Technology Company, Crowdstrike says that their security software called 'Falcon Platform' uses Ai technology to safeguard against ransomware threat and risk. The cyber security software uses anomaly detection for end-point security in their enterprise networks.

- **#5. Email Monitoring –**
  Businesses have to understand the importance of monitoring email conversation to avoid Cybersecurity hackings such as phishing. ML-based monitoring software can now help speed up the detection of cyber threats and develop detection accuracy.
- A wide range of AI technologies is used for monitoring. For example, some software will use email to view email, to see if the email contains any features that indicate threats, like pictures of a specific size.
- In other cases, NLP (Natural Language Processing) will be used to read the text through incoming and outgoing emails to identify patterns or phrases in the message associated with phishing efforts. Business can find whether the email recipient, sender, attachment, or body is threatened, by using anomaly detection software.
- **Example:**
  A famous software company in London, Tessian offer email monitoring AI software that helps financial institutions to prevent phishing attacks, misdirected emails, and data breaches.
  Tessian's software uses anomaly detection and NLP at various stages to recognize which emails are Cybersecurity threats.

USING ML AGAINST SMS SCAMS

- The SMS Spam problem is increasing nowadays with the increase in the use of text messaging. SMS Spam filtering is a big challenge these days.
- Hackers using the umbrella moniker “COVID-19” are phishing and defrauding people via SMS and internet-based texting services like WhatsApp and Telegram.
- The MTD system (Mobile Threat Défense System) is employed in this Machine Learning use case. In this case, machine learning algorithms are able to separate the hackers from real Covid-19 signals.
- Different endpoints, such as mobile phones, laptops, and computers, have protection. The Unified Endpoint Management application keeps them safe. Text-based applications and SMSs benefit greatly from UEM. The model is trained with a variety of datasets to recognize threats amid genuine messages.
- Technique for SMS Spam filtering can be used based on 10 features using five machine learning algorithms namely Naïve Bayes, Logistic Regression, J48, Decision Table, and Random Forest.
- Refer https://www.researchgate.net/publication/318657353_Towards_Filtering_of_SMS_Spam_Messages_Using_Machine_Learning_Based_Technique

USING ML FOR SECURING MOBILE ENDPOINTS

- Data privacy, security fixes, and anti-virus programs all use machine learning, whether on iOS or Android.
- Machine Learning is already being implied by Google in mobile device security.
- In networks, devices, and vulnerability assessment tools, machine learning is able to prevent cyber threats.
- Personal AI-driven assistance is provided through Apple's Siri, Google Assistant, and Amazon's Alexa. They are in charge of protecting voice-based commands using machine learning. Also, to distinguish the true owner's voice from that of a hacker.
- Wandera, a cybersecurity leader, employs its machine learning system. They discovered 500 ransomware strains on the commercial mobile devices of several companies.
- With a constant stream of signals coming in, a model can be built that is continually processing and fine-tuning the baseline. This allows for more dynamic security decisions, ability to detect real-time threats, and, even more importantly, tailor the security response to the present context.

APPLICATIONS OF MACHINE LEARNING IN CYBERSECURITY:

EXAMPLES OF MACHINE LEARNING IN CYBERSECURITY

1. Spear Phishing:

- Orthodox phishing prevention strategies are less in speed and hence, less accurate in locating all the suspicious connections leaving users at risk.
- The solution to this issue lies in the models of predictive URL detection focused on the new machine learning algorithms that can discover patterns that expose the email of a malicious sender.
- Such models are ready to understand small-scale activities such as email headers, body data, models, etc. From these prepared templates, it is possible to identify whether or not the email is malicious.

APPLICATIONS OF MACHINE LEARNING IN CYBERSECURITY:

EXAMPLES OF MACHINE LEARNING IN CYBERSECURITY

2. **Watering Hole**

- A watering hole attack is a form of cyberattack that targets groups of users by infecting websites that they commonly visit.
- Programmers are aiming to map the places often accessed by users that are beyond the private arrangement of a person.
- By observing the way the web traverses, machine learning algorithms will maintain the security level of the internet application administration.
- It will differentiate whether customers are connected to malicious websites when traveling along the target route.
- In order to describe these malicious spaces, machine learning system traversal discovery algorithms can be used. In addition, machine learning can scan for odd or unusual diverting designs to and from the host of a site.

APPLICATIONS OF MACHINE LEARNING IN CYBERSECURITY:

EXAMPLES OF MACHINE LEARNING IN CYBERSECURITY

3. **Webshell**

- It is a piece of code that is maliciously piled on an online platform in order to allow the attacker to make modifications to the server's Internet root catalog.
- This ensures that the framework's complete access to the database is collected. In the event that it is an e-commerce platform, in order to obtain credit card information from the customer base, attackers might get to the website on a visit basis.
- Machine learning makes it possible to detect statistics of normal shopping cart activity and to train machine learning models to distinguish normal behaviors from malicious behavior.
- To train the model further, detected malicious files could be executed on a supervised standalone device. It is possible to use these machine learning algorithms to recognize web shells pre-emptively and separate them from the system until they manipulate the system.

APPLICATIONS OF MACHINE LEARNING IN CYBERSECURITY:

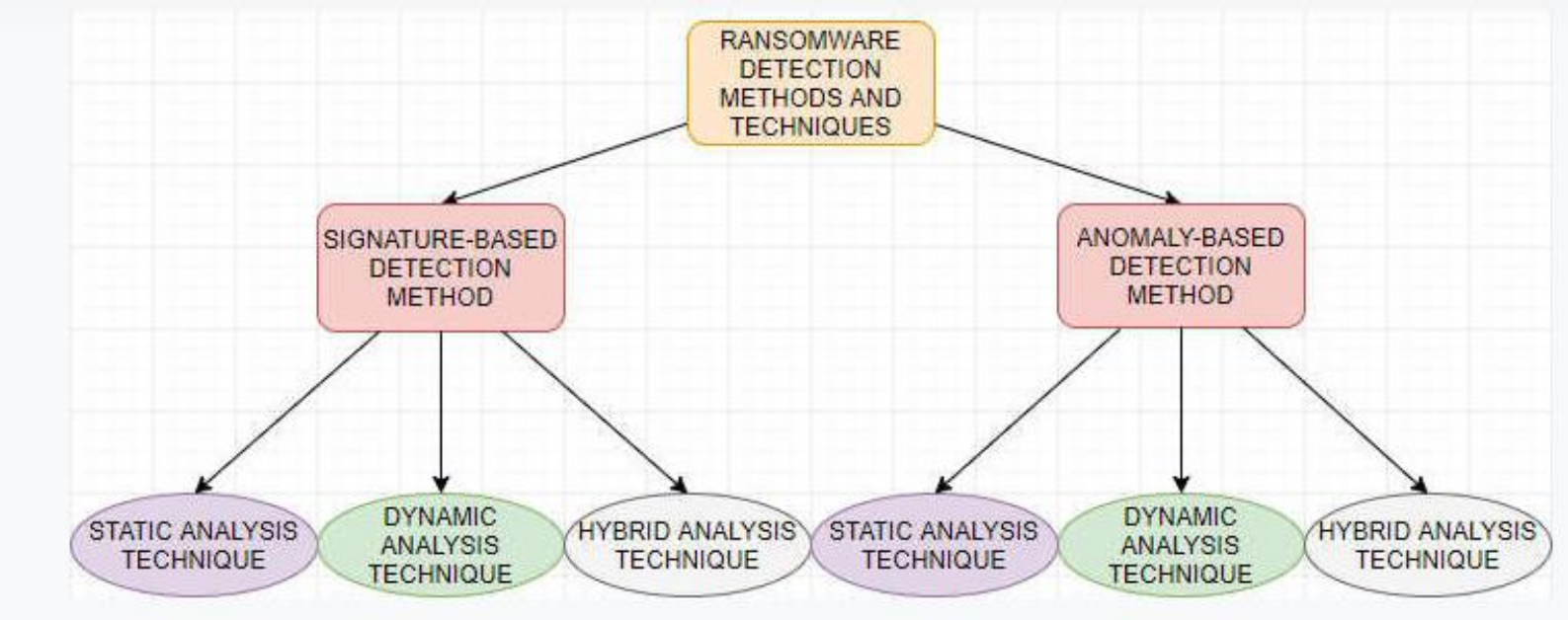
EXAMPLES OF MACHINE LEARNING IN CYBERSECURITY

4. **Ransomware**

- A mixture of ransom + software could be ransomware.
- It applies to some type of automated program that demands the encryption key of the user's stolen records for any sort of ransom in exchange.
- The encryption key is basically a key for the recipient to unlock the bolted documents. Mixed media documents, official records, or framework records that a user's machine relies upon could be bolted records. Ransomware is available in 2 forms:

- Record coder that scrambles documents (changes to mystery code over info).
- The Bolt screen locks a computer and forbids the user from using it until it pays for the delivery.

- Ransomware detection using Machine Learning (ML)
- There are many different machine learning mechanisms that are used today for both detecting and protecting your data from a ransomware infection. However, many of the current means used are considered to be a legacy at this point.



- **Signature**-based detection was the de facto standard at detecting malware threats. The signature-based protection works off the premise of having a signature that covers the specific malware to know how to detect the threat.
- Machine Learning is used to build behavioral analytics systems that are trained to detect anomalous file behavior. These systems provide a great way to recognize and stop ransomware infections from progressing through the file system. Solutions that make use of ML are able to recognize anomalies in file behavior that may include changes being made by ransomware.

APPLICATIONS OF MACHINE LEARNING IN CYBERSECURITY:

EXAMPLES OF MACHINE LEARNING IN CYBERSECURITY

5. **Remote exploitation**

- A pernicious behavior that attacks or organizes machines can also be referred to as a remote intruder.
- The attacker picks up the frame from the defenceless attention of the computer or entity.
- The aims of a remote attack are to misuse and delete touchy information from the system or to disrupt the machine-focused entity by presenting a malicious computer application. In various ways, remote manipulation will happen:

6. **Denial of service attack:**

- Usually, by overwhelming the servers with untrue client requests, a technique to make the site unavailable to clients.
- It causes a massive usage surge that solidifies servers and concerns them about proceeding with a huge amount of pending demands.

APPLICATIONS OF MACHINE LEARNING IN CYBERSECURITY:

EXAMPLES OF MACHINE LEARNING IN CYBERSECURITY

7. DNS poisoning: To compare numeric IP addresses, DNS servers are frameworks that view human-memorable space names like facebook.com.

To identify and accept properties on the network, DNS mechanisms are used. Fundamentally, hurting DNS servers means deceiving them to accept misrepresented beginnings of knowledge as real and diverting clients that get to those damaged DNS servers to locations that unintentionally download malicious programs or pathogens through the system.

8. Port scanning: Device ports are used for information transmission and retrieval. Port scanners may be used to discern knowledge vulnerabilities and pick up machines and monitor them by abusing certain vulnerabilities.

THANK YOU