**CSCI 538 Assignment 01Literature**

**Review and Case Study**

**BHARATH REDDY YEMAPALLA**

**CWID -50322318**

**Q 1.**

**(A)**

There are many specific AI computer systems and tools used in cybersecurity to enhance security measures, detect threats, and respond to cyberattacks. Two notable examples of AI-driven cybersecurity tools are:

**IBM QRadar**: IBM QRadar is a security information and event management (SIEM) tool that uses artificial intelligence (AI) and machine learning to track and examine security data from diverse sources. It can identify potential security threats, anomalies, and suspicious activity in real-time. In order to correlate data and produce insights, QRadar leverages AI. As a result, security teams are better able to recognize and address security events.

**Darktrace:** Darktrace is a machine learning-powered cybersecurity tool that uses AI to identify and address online threats. It uses "self-learning AI" technology to comprehend the typical endpoint and network behavior of an enterprise. Darktrace can detect variations from this baseline and identify prospective dangers, such as insider threats and developing assaults, enabling proactive threat mitigation.

These equipment, coupled.

**(B)x**

Cybersecurity, in a broad sense, does not directly control satellites or diagnose photocopiers, but it is essential in defending computer systems, networks, and data against illegal access, breaches, and threats. It makes sure that digital assets are private, trustworthy, and readily available. Three of the primary purposes of cybersecurity programs are as follows:

**Managing access**

Authentication: Cybersecurity applications authenticate users' and their equipment's identities before allowing them access to a system or network. Utilizing two-factor authentication, biometrics, or passwords are some examples of this.

Authorization: Once a user or device has been authenticated, cybersecurity controls outline the type of access they should have. For various users or jobs, this also entails setting up permissions and privileges.

Account management: Managing user accounts, which includes setting up, altering, and deleting them as necessary, is an essential task. This

**Management of Vulnerabilities**

Cybersecurity technologies examine networks and systems for vulnerabilities, or weak spots that an attacker could use to their advantage. They locate weaknesses in programs, settings, or hardware.

Patch management: After vulnerabilities are found, cybersecurity programs help with the installation of patches and updates to correct them. By correcting known weaknesses, this aids in keeping systems secure.

Threat Intelligence: A lot of cybersecurity products integrate threat intelligence feeds to stay current on new threats and vulnerabilities, enabling enterprises to proactively protect against them.

**Detecting threats and taking action:**

Intrusion Detection and Prevention: These tools keep an eye on system logs and network traffic for indications of malicious or suspicious activities. They have the ability to instantly block or warn administrators of potential risks.

Cybersecurity programs assist firms in successfully responding to security incidents when they happen. They make it easier to conduct investigations, contain threats, eliminate them, and recover.

Forensics and Analysis: Following a breach, cybersecurity technologies help with forensic analysis to determine the extent of the occurrence, acquire proof, and support legal or disciplinary proceedings.

The protection of digital environments and the avoidance of illegal access and data breaches are all made possible by cybersecurity. Depending on the tools and technology employed, cybersecurity programs can perform a variety of specific tasks, but these tasks offer a basic framework for safeguarding digital assets.

**(C)**

In order to identify and reduce threats, AI technologies in cybersecurity use a variety of methods and methodologies. In addition to descriptions of the data they employ, the following are the three key AI technologies that are frequently used in cybersecurity:

Computer learning (ML):

Supervised Learning: Machine learning (ML) models are trained on labeled datasets including instances of both legitimate and harmful activity. For instance, supervised ML models can be trained using samples of known malware and safe software. Once taught, it can categorize fresh instances as malicious or benign using recognized patterns.

Unsupervised Learning: In this scenario, ML models locate patterns or irregularities in data without the aid of labeled samples. In network traffic, user activity, or system records, anomaly detection algorithms can identify differences from expected behavior.

ML models frequently rely on feature engineering.

**Processing of natural language (NLP):**

Text Analysis: Text-based data, such as emails, chat logs, social media posts, and security-related documents, are analyzed using NLP algorithms. Identification of security-related debates and threats can be aided by sentiment analysis, topic modeling, and named entity recognition.

Phishing Detection: NLP models can examine email content and find suspicious patterns, links, or language to identify phishing attempts.

Text-Based Threat Intelligence: NLP is employed to parse and extract important data from unstructured sources, such as security blogs, forums, and news stories, in order to stay up to date on new risks.

**To learn deeply:**

CNNs (Convolutional Neural Networks): CNNs are used for image-based cybersecurity tasks like assessing network traffic visualizations or finding malware in file samples. They can pick up on patterns in visual information.

Recurrent neural networks (RNNs): RNNs are used to analyze sequential data, such as network traffic or time-series logs. They can detect irregular sequences of events and capture temporal connections.

Generative Adversarial Networks (GANs): GANs are capable of generating adversarial examples that can be used to evaluate the sturdiness of security systems that use AI. They aid in enhancing cybersecurity systems' robustness.

**RL: Reinforcement Learning**

RL algorithms can interact with a simulated environment or network to learn the best security policies. They can be applied to real-time threat response or network access decisions.

Security that may be adjusted dynamically in response to threats and network conditions is known as adaptive security (RL). In reaction to shifting threat environments, it could, for instance, modify firewall rules or access constraints.

**Analytical graphs**

Cybersecurity typically entails examining connections between elements (such as users, devices, and IP addresses) in a network. This is known as "graph-based threat analysis." In these intricate networks, anomalies or suspicious connections might be found with the aid of graph analytics.

Threat Attribution: Graph analytics can help identify individual threat groups or nation-states responsible for assaults by mapping the infrastructure and strategies they deploy.

There are many different types of data that can be used in cybersecurity AI applications, including network traffic logs, system event logs, firewall data, DNS logs, malware samples, threat intelligence feeds, text-based data (emails, logs, reports), and even data from external sources like social media. In order for AI models to produce accurate forecasts and recognize abnormalities and dangers, these datasets are essential for developing and testing them.

**(D)**

Depending on the exact application, the caliber of the data, the complexity of the AI algorithms, and the environment in which they are utilized, the performance of AI technologies in cybersecurity might vary greatly. An overview of how AI in cybersecurity typically functions is provided below:

**In contrast to humans:**

Scalability and speed: AI systems are able to process enormous volumes of data quickly and make judgments in real-time, which is not possible for humans. They can monitor network traffic quickly, spot patterns, and react to hazards more swiftly than human operators.

Consistency: AI systems provide a high degree of operational consistency, ensuring that security regulations are enforced consistently throughout an organization.

extensive Analysis: Without getting weary, AI can perform extensive analysis, searching through enormous databases for abnormalities or vulnerabilities.

**Prevention and Detection**

Malware detection: AI-based antivirus and anti-malware programs frequently outperform conventional signature-based systems at spotting new and undiscovered threats.

Anomaly Detection: AI-enhanced anomaly detection can spot odd patterns or behaviors in network traffic, user activity, or system records that people might overlook.

Detection of Phishing: AI can help in detecting phishing attempts by looking at email content and sender activity.

**Problems and Restrictions:**

False Positives: AI systems have the potential to produce false positives that identify harmless actions as dangers, making it time-consuming for security professionals to look into them.

Adversarial assaults: By designing assaults designed to get around AI-based detection systems, attackers can take advantage of their weaknesses.

Contextual Understanding: AI may have difficulty understanding the context of an event or behavior. As a result, it may not always be able to do so.

**Assessment and Validation:**

Metrics including true positives, false positives, false negatives, precision, recall, and F1-score are frequently used in cybersecurity to assess AI performance.

AI systems are updated frequently and tested against fresh threats. Exercises known as "red teams," in which ethical hackers assess the efficacy of AI security solutions, are also frequent.

**Working together with AI:**

Collaboration between humans and AI is frequently the most successful strategy. Routine jobs can be automated with AI's help, and it can quickly identify and respond to recognized risks while human analysts add crucial context, look into complicated occurrences, and make strategic judgments.

**Considerations for Regulatory and Compliance:**

When applying AI to cybersecurity, businesses must take regulatory and compliance standards into account. Some regulations call for human review of AI decisions.

In conclusion, AI technologies have made great strides toward improving cybersecurity, especially in terms of speed, scalability, and the capacity to process massive amounts of data. However, they should not be utilized in place of human knowledge because they are not a cure-all. Thorough testing and evaluation are essential to ensure that AI's performance satisfies the organization's security objectives because AI's efficacy in cybersecurity is always changing as both the technology and threat landscape evolve.

**(E)**

The phrase "AI in cybersecurity" refers to a wide range of applications, tools, and systems, some of which are under development and have already seen widespread use in the market. A program may be in various states at any given time. Let's examine the potential outcomes:

**Cybersecurity with experimental AI**

Research labs, academic institutions, and start-up businesses frequently create experimental programs. Although not yet commonly used in the industry, they might be innovative.

Few companies or researchers may be using experimental AI cybersecurity solutions for testing or study.

A high level of technical competence in both AI and cybersecurity is frequently required of users of experimental AI cybersecurity products. They are frequently academics or industry leaders.

**AI in the Field for Cybersecurity**

Programs that have been "fielded"—i.e., designed, tested, and put into use by organizations—are those that have been used in actual cybersecurity environments.

Usage: A wide range of enterprises, including businesses, governments, and providers of critical infrastructure, use fielded AI cybersecurity solutions.

User competence: Depending on the particular solution, different levels of user competence may be needed. A security professional with a moderate level of technical expertise can use some solutions because they are user-friendly in design. Others might need more specialized knowledge, particularly for setting and modification.

Solutions for commercial AI security:

There are many well-known cybersecurity businesses that provide extensively used AI-driven security goods and services.

Use: Many companies throughout the world use commercial AI security solutions.

User Expertise: The level of experience needed can change. Various levels of technical expertise can use some commercial solutions because they are made to be simple to use. Others might need specific instruction.

**Tools for Open-Source AI Security:**

A large community of users and developers can use some AI cybersecurity technologies since they are open-source.

Usage: A variety of businesses, even those with little resources, can use open-source AI security products.

User knowledge: Depending on the tool, different levels of knowledge are needed. While some open-source programs are simple to use, others could require more technical skill.

In conclusion, the level of AI in cybersecurity programs can range from cutting-edge research initiatives to extensively used commercial solutions. Depending on the program's development and accessibility, the user base can vary greatly. The level of user expertise varies as well, with some solutions being simple enough for non-experts to use and others being developed for cybersecurity experts with high-level technical skills.

**(F)**

Because it demonstrates a number of traits common to intelligent systems, artificial intelligence in cybersecurity is regarded as intelligent.

**Adaptability**: Intelligent AI cybersecurity systems are able to change with the dangers and surroundings they operate in. They gain knowledge from past experiences and can modify their tactics and reactions accordingly. For instance, they can recognize fresh varieties of malware or attack tactics that they haven't seen previously.

Cybersecurity systems powered by AI can learn from data. They can spot trends, anomalies, and patterns in huge datasets by using machine learning algorithms. Based on the knowledge they have gained, they are now able to foresee the future and make judgments.

**Automation**: In the field of cybersecurity, intelligent AI systems are capable of automating a number of processes, including threat detection, incident response, and security policy enforcement. They can complete these jobs without ongoing human supervision, increasing productivity and speed.

AI cybersecurity systems are excellent at seeing intricate patterns in data, such as network traffic, user behavior, or virus signatures. They are able to spot odd patterns that can point to security risks.

Data analysis in real-time is a feature of many AI cybersecurity solutions. They can respond to threats right away thanks to this capacity, which narrows their window of vulnerability.

**Anomaly Detection:** AI systems that are intelligent can identify abnormalities or departures from normal behavior. Even if certain actions haven't been formally classified as threats, they can nonetheless spot questionable or potentially dangerous behavior.

**Scalability**: AI cybersecurity systems have the potential to scale their operations to manage high data and network traffic volumes. In today's data-rich situations, their ability to process and analyze large datasets is crucial.

Continuous Improvement is a possibility for machine learning models used in cybersecurity. As dangers change, they can adjust and retrain, growing more potent over time.

**Multimodal Data Analysis**: Intelligent systems have the ability to examine a variety of data formats, including text, graphics, network traffic, and log files. To make better security decisions, they might combine data from many sources.

Collaboration between humans and AI: Many cybersecurity AI systems are built to work with human analysts. They can offer information, rank alerts, and support analysts' decision-making, improving the overall security posture.

AI systems are capable of conducting behavioral analysis, which involves observing how users and other network elements normally behave. By doing so, they are able to spot variations from the norm that may be a sign of compromised accounts or insider threats.

Some highly developed AI systems are capable of comprehending context. They can take into account the larger context of security events and incidents and decide if an activity is a real threat or a false positive with more knowledge.

AI in cybersecurity is intelligent due to the combination of these features. Even while they might not have general intelligence comparable to that of a human, AI systems show specialized intelligence when it comes to identifying, evaluating, and addressing cybersecurity threats and difficulties.

**(G)**

Depending on the particular application, business, and development team, different programming languages and environments can be used to develop AI in cybersecurity systems. However, there are a few standard programming languages, settings, and user interface factors to take into account:

Scripting Languages

**Python**: Machine learning and AI applications in cybersecurity frequently employ Python. It includes a robust ecosystem of tools and libraries, including popular ones for creating AI models like TensorFlow, PyTorch, and Scikit-learn.

Java: Another popular option is Java, particularly for creating network monitoring tools and security apps. It is renowned for being durable and portable.

**C/C++:** These programming languages are used for cybersecurity systems' performance-critical parts, like malware analysis and low-level packet processing.

R: R is utilized in data visualization and statistical analysis in Cybersecurity.

**Environments for Development:**

Jupyter Notebooks: Jupyter is a well-liked platform for constructing machine learning models and experimenting new ideas. Data visualization and interactive coding are also possible.

Integrated Development Environments (IDEs): Depending on their preferred language, developers frequently utilize IDEs like PyCharm, Visual Studio Code, or IntelliJ IDEA.

Custom Development Environments: Depending on their unique requirements and work processes, some businesses create custom environments.

**the user interfaces**

Security experts prefer command-line interfaces (CLIs) because of their effectiveness and adaptability, which are included in many cybersecurity products and scripts.

Graphical User Interfaces (GUIs): Some AI-driven cybersecurity solutions, especially those intended for non-technical users, may have GUIs that offer comprehensible dashboards and visualizations.

Web interfaces: Users can access and manage AI-driven security features through web browsers thanks to web-based interfaces, which are typical for security management platforms.

APIs: AI cybersecurity systems frequently expose APIs (Application Programming Interfaces) for automating programmatic access to security tools and procedures.

The specific use case, the team's skill set, and the intended audience are all important considerations when choosing a programming language and environment. Systems using AI in cybersecurity can include a variety of user interfaces to accommodate various user roles and preferences, from technical professionals who prefer command-line tools to non-technical users who want intuitive GUIs.

**(H)**

https://renaissancerachel.com/best-ai-security-tools/

https://drexel.edu/cci/stories/role-of-AI-in-cybersecurity/

https://en.wikipedia.org/wiki/Artificial\_intelligence

drexel

https://www.trustage.com/business-solutions/business-protection/cybersecurity-protection?utm\_source=google&utm\_medium=cpc&utm\_campaign=NB\_sbt-external-activation\_BZP\_B2B&utm\_term=cybersecurity&utm\_content=&gclid=EAIaIQobChMI1PD1zoGzgQMVVkp\_AB0D3A-7EAAYASAAEgJKzfD\_BwE

https://www.techtarget.com/searchsecurity/definition/cybersecurity

https://www.balbix.com/insights/artificial-intelligence-in-cybersecurity/

https://www.springboard.com/blog/cybersecurity/best-programming-language-for-cybersecurity/

**Q 2.**

Based on the definitions of artificial intelligence and agents learned in your lectures, here is an assessment of the extent to which the following cases of a computer system qualify as AI:

**a) Supermarket barcode readers:**

AI Degree: Limited AI

Explanation: Supermarket barcodes are designed for a specific task - to read barcodes and look up product information in the database. They lack general intelligence and do not adapt to new tasks. They are more than specialized automated systems.

**b) Voice controlled telephone menus:**

AI Degree: Limited AI

Explanation: Voice-activated telephone menus, often called interactive voice response (IVR) systems, understand spoken language to some extent, but typically follow predefined decision trees and are rule-based. They have no real understanding or reasoning and operate in a certain field.

**(c) The spelling and grammar correction functions of Microsoft Word:**

AI Degree: Weak AI

Explanation. Spelling and grammar correction features in word processing programs such as Microsoft Word use algorithms to detect errors and recommend corrections. Although they can offer useful suggestions, they lack general intelligence. They rely on rule-based and statistical methods to improve text quality.

**d) Internet routing algorithms that dynamically respond to the network state:**

AI Degree: Limited AI

Explanation: Internet routing algorithms are designed to make routing decisions based on network conditions such as congestion or link failures. Although they have adaptive behavior, they lack general intelligence. These algorithms are usually rule-based and designed to optimize network traffic flow.

**(e) Virtual assistants such as Siri, Google Assistant and Alexa:**

AI Degree: Strong AI (Narrow AI)

Explanation: Virtual assistants such as Siri, Google Assistant and Alexa demonstrate higher levels of artificial intelligence. They use natural language processing (NLP) and machine learning to understand and respond to spoken or written questions, perform tasks such as setting reminders, answering questions and controlling smart devices. Although they are not sentient, they can adapt to a wide range of user interactions and tasks, making them examples of niche or specialized AI.

**Q 03.**

**(a) PEAS Task Environment Description:**

**Performance Measure:** The capacity of the thermostat agent to keep the temperature within 3 degrees of the target setting—neither too hot nor too cold—while consuming the least amount of energy, is how well it performs.

**Environment:** The HVAC (Heating, Ventilation, and Air Conditioning) system, specifically the Air Conditioner (AC), and the actual room or area where the thermostat is situated make up the environment.

**Actuators**: In this setting, the air conditioner's controls are the actuators. Depending on the temperature reading and the chosen setting, the thermostat agent can switch the AC on or off.

**Sensors**: The sensors consist of a temperature sensor to determine the room's current temperature and a user input device to establish the preferred temperature.

**(b) Environment Characterization:**

The following characteristics can be used to describe the environment:

Because the thermostat agent can only directly monitor the present room temperature, the environment is only partially observable. It cannot see things like the outside temperature or the condition of the HVAC system immediately.

The thermostat agent's activities directly influence the room's temperature, making the environment predictable. The consequences can be predicted if the thermostat agent turns on the air conditioning when it is too hot and turns it off when it is too cold.

The environment is episodic because the agent's decisions (such as whether to turn the AC on or off) are dependent on the current situation (such as the temperature of the room) and not on the course of earlier decisions or events or states.

**Static**: Because the environment doesn't change on its own, it can be said to be static. The agent's actions are what cause the temperature variations.

**Discrete**: The thermostat agent functions with discrete actions (turning the AC on or off) based on discrete temperature data and settings, making the environment discrete.

**(c) Total Number of Potential States**

The granularity of temperature measurements and settings determines the number of potential states in the state space. We have a state space with (Temperature Range / Granularity) + 1 potential states if we assume that temperature measurements are made to the nearest degree and that settings are made to the nearest degree. For instance, there are (80 - 60) + 1 = 21 potential states if the temperature range is 60°F to 80°F and the granularity is 1°F.

**(d) Agent category:**

An illustration of a straightforward reflex agent is the thermostat. This is why:

Simple Reflex Agent: Based just on the current percept (temperature reading) and a specified criterion (temperature being at least 3 degrees below or above the setting), the thermostat decides whether to switch on or off the air conditioning. It doesn't fully internalize the surroundings or take long-term effects into account. It just responds to the situation as it is at the moment.

In contrast, more complex decision-making methods would be required for other sorts of agents, such as model-based reflex agents, goal-based agents, utility-based agents, or learning agents, which would optimise some utility function or take into account past data. The thermostat's activities are rather straightforward and closely related to a certain state in the environment