AI-driven Cybersecurity

based on **AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions**

What is Cybersecurity

Cybersecurity involves the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes. Cybersecurity uses technologies, processes, and controls to protect systems, networks, programs, devices, and data from cyberattacks. It aims to reduce the risk of cyberattacks and protect against the unauthorized exploitation of systems, networks, and technologies.

Limitations of Traditional Security Solutions

Traditional security solutions such as antivirus software, firewalls, user authentication, and encryption, while still necessary, are increasingly inadequate to meet the complex and evolving needs of today's cybersecurity landscape. The key problem with these systems is their reliance on manual operation by a limited number of experienced security experts, leading to ad-hoc data processing that lacks the capability to run intelligently and adaptively.

AI based security intelligence modeling

- NLP (natural language processing)
- KRR (knowledge representation and reasoning)

NLP

- Using natural language processing model
- Natural Language Processing (NLP) is considered as an important branch of AI that can make it possible for computers to understand human language, interpret it, and eventually determine which parts are important in an intelligent system
- NLP's ultimate aim is to extract knowledge from unstructured data or information, i.e., to interpret, decipher, comprehend, and make sense of human languages in a valuable way.

Parts Of NLP

- Lexical analysis
- Syntactic analysis
- Semantic analysis

Lexical Analysis

Lexical analysis It usually includes the arrangement of terms being described and analyzed. Lexical analysis separates the entire chunk of text according to the criteria into paragraphs, sentences, phrases, or tokens such as identifier, keyword, literal, etc.

Consider a scenario where a cybersecurity team is trying to identify and block phishing websites. Phishing websites often use domain names that mimic legitimate websites, but with subtle differences. By applying lexical analysis, the team can break down and analyze the text of these domain names to identify patterns and characteristics typical of phishing attempts.

- Example: An email contains the sentence: "Dear user, your account has been compromised. Please visit www.bank-secure.com to verify your identity. "Tokens: ["Dear", "user", "your", "account", "has", "been", "compromised", "Please", "visit", "www.bank-secure.com", "to", "verify", "your", "identity"]
- In general, Lexical analysis is the first phase of a compiler or interpreter for programming languages. It involves scanning the source code to convert sequences of characters into meaningful tokens.

Syntactic analysis

It is seen as one of the key tools used to complete the tasks of the NLP, which is used to determine how the natural language aligns with the grammatical rules.

Consider a cybersecurity firm that wants to predict and prevent cyberattacks by analyzing threat intelligence reports and social media feeds for emerging threats. These texts often contain valuable information but are unstructured and require syntactic analysis to extract meaningful insights.

Example: Parsing the sentence: "Dear user, your account has been compromised. Please visit www.bank-secure.com to verify your identity."

- Subject: "your account"
- Verb: "has been compromised"
- Action: "Please visit"
- Object: "www.bank-secure.com"
- Purpose: "to verify your identity"

Semantic analysis

Semantic analysis Another of the key methods used to complete NLP assignments is semantic analysis, which includes understanding the context and perception of words and how sentences are structured.

Semantic analysis is used to understand the context and meaning of the sentence. Techniques like latent semantic analysis (LSA) and named entity recognition (NER) are applied to extract deeper insights and recognize entities.

- Techniques like latent semantic analysis (LSA) and named entity recognition (NER) are applied to extract deeper insights and recognize entities.
- Example**:** Using LSA and NER on the parsed sentence to identify keywords and entities:
- LSA identifies key phrases: "account compromised," "verify your identity"
- NER recognizes entities: "user" (person), "www.bank-secure.com" (URL), "account" (financial term)
- Contextual Understanding**:** The semantic analysis understands that the phrase "account has been compromised" often indicates a phishing attempt, especially when followed by a call to action like "Please visit www.bank-secure.com to verify your identity." Recognizing "www.bank-secure.com" as a URL and "verify your identity" as a sensitive request helps classify this email as potentially malicious.

Application of NLP

- Detecting malicious domain names
- Vulnerability analysis
- Phishing identification
- Malware family analysis

Detecting Malicious Domain Names

Scenario: An organization notices an unusual increase in traffic to a suspicious domain, "clbwpvdyztoepfua.lu".

NLP Application: Using NLP techniques, security systems analyze domain names in DNS traffic to detect patterns typical of malicious domains (random strings of characters, uncommon domain extensions, etc.).

Real-Life Example: A cybersecurity firm sets up an NLP-based system that identifies and blocks domains like "clbwpvdyztoepfua.lu" by comparing them to a dataset of known benign domains (e.g., cnn.com). This prevents employees from accessing phishing sites disguised as legitimate ones.

Vulnerability Analysis

Scenario: A financial institution is concerned about the possibility of zero-day vulnerabilities in its software.

NLP Application: Analysts use NLP techniques like n-grams and smoothing algorithms to scan code repositories and discussions on developer forums for patterns indicative of vulnerabilities.

Real-Life Example: Security researchers at a bank utilize an NLP model to analyze code commits and bug reports. They identify a vulnerability similar to those discussed in hacker forums and patch it before it can be exploited, thus preventing a potential security breach.

Phishing Identification

- Scenario: Employees of a company receive an email that appears to be from their IT department, asking them to reset their passwords.
- NLP Application: An NLP-based machine learning model analyzes the email content, webpage layout, and URL structure to detect phishing attempts.
- Real-Life Example: A company's cybersecurity system uses NLP to examine emails for phishing indicators such as urgent language, suspicious links, and unusual senders. It flags and quarantines an email with a URL redirecting to a fake login page, preventing employees from entering their credentials into a phishing site.

Malware family analysis

- Scenario: A new type of malware is spreading rapidly and affecting various organizations.
- NLP Application: Security experts model behavioral reports of the malware as a series of words using a bag-of-words (BoW) approach, then use NLP to detect and classify malware.
- Real-Life Example: A cybersecurity firm receives reports of a new malware variant. They employ An NLP-based BoW model to analyze the behavioral patterns described in incident reports. This helps them quickly classify the malware as part of the "Trojan" family, allowing them to deploy appropriate countermeasures to affected systems.

Knowledge Representation and Reasoning

- Representation of Real-World Information: Ensures intelligent systems can use this information like humans. Facilitates problem-solving for complex security issues.
- Analysis: Focuses on how a cybersecurity agent's views, intentions, and decisions can be articulated for automated reasoning.
- Complex Problem Solving: Helps intelligent systems solve complex security problems similarly to how humans would. Enables systems to understand and analyze vast amounts of security-related information.
- Automated Reasoning: Allows for the use of inference engines and classifiers to automate the reasoning process. Facilitates quicker and more accurate decision-making in cybersecurity.
- To create knowledge-based conceptual model several knowledge representation methods are used as discussed further

Knowledge Representation Methods

- Logical representation
- Semantic network representation
- Frame representation
- Production rules

Logical representation

- It represents with concrete rules without any ambiguity that typically deals with propositions. Thus, logic can be used to represent simple facts that are the general statements that may be either ‘True’ or ‘False’.

- Overall, logical representation means drawing a conclusion based on various conditions.

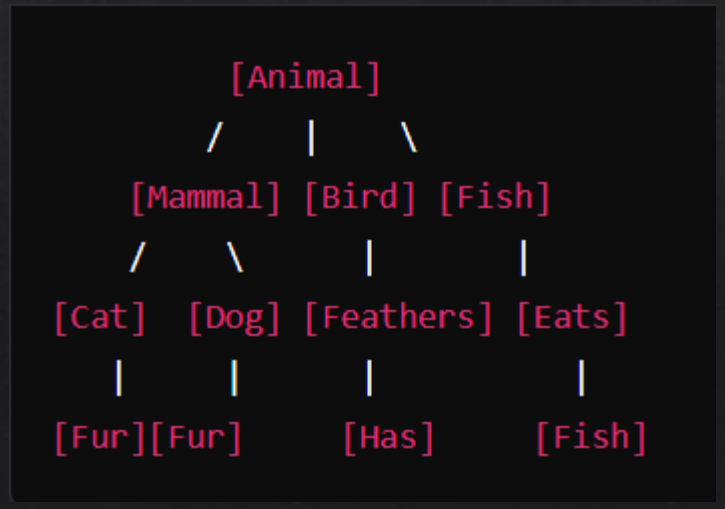
Production rules

- Production rules It typically consists of pairs of the condition, and corresponding action, which means, “If condition then action”.
- The main advantage of such a rule-based system in cybersecurity is that the “condition” part can determine which rule is suitable to apply for a specific security problem.
- For example: Condition: If the network traffic exceeds a certain threshold.

  Action: Block the IP address generating the excessive traffic.

Semantic network representation

- We may represent our information in the form of graphical networks within semantic networks. This network is made up of objects and arcs representing nodes that define the relationship between those objects.
- Nodes are objects
- Arcs are relation between objects



Frame representation

- A frame, derived from semantic networks, is a structure-like record that consists of a set of attributes to represent an object in the world and its values.
- Although frame representation is easy to understand and visualize, it cannot proceed with the inference mechanism smoothly.

Frame: Dog

Attributes (Slots)	Values
Type	Mammal
Species	Canis lupus familiaris
Color	Various
Sound	Bark
Owner	John Doe
Age	3 years
Vaccinated	Yes

What are Security Ontologies

- In general, ontology is “an explicit specification of conceptualization and a formal way to define the semantics of knowledge and data”
- We use Security Ontologies to make the knowledge-based conceptual model by establishing relation between knowledge and the data present

Components of Ontology

- Concepts (C): Represent entities or ideas in the domain (e.g., "Animal," "Car").
- Relations (R): Define how concepts are related (e.g., "is a," "part of").
- Instances (I): Specific examples or instances of concepts (e.g., "Fluffy" as an instance of "Cat").
- Hierarchy (H): Organizes concepts into a hierarchical structure (e.g., "Cat" is a subclass of "Animal").
- Axioms (A): Additional rules or constraints that define the behavior or characteristics within the ontology.

How Ontologies Work

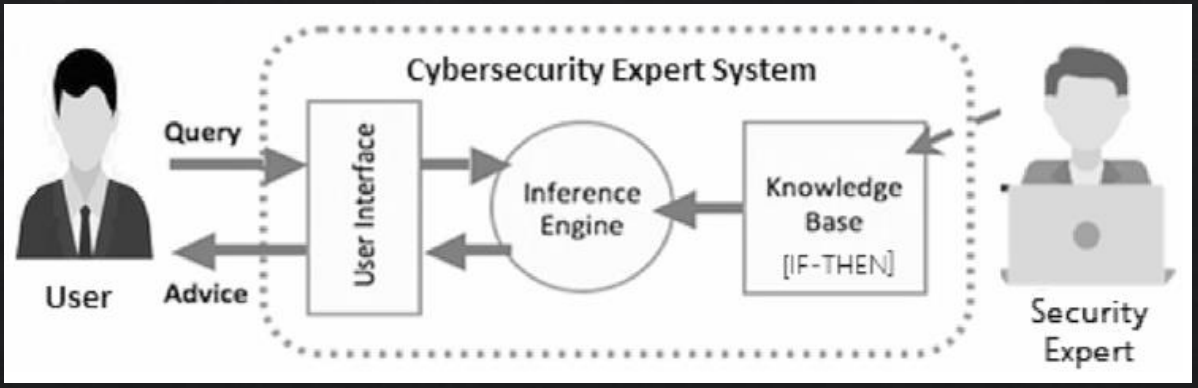
- Definition: Ontologies start by defining concepts (like "Animal"), their properties (like "has fur"), and relationships between them (like "is a" or "part of").
- Hierarchy: Concepts are often organized hierarchically, where more specific concepts (like "Cat") inherit characteristics from more general ones (like "Animal").
- Instance Handling: Instances (specific examples) of concepts (like "Fluffy" as a specific cat) are categorized within the ontology.
- Usage: Systems or applications can utilize ontologies to structure data, classify information, and perform tasks like search, inference, or decision-making based on the defined rules and relationships.

Concept of security based Ontology

- Concept: Threat represents various types of difficulties or dangers against a given set of security properties.
- Concept: Vulnerability mainly represents the weaknesses of a cybersecurity system.
- Concept: Attack represents various types of security incidents caused by cyber criminals.
- Concept: Impact represents the effects that a security incident can imply.
- Concept: Controls represents the relevant mechanisms that can be used to reduce or avoid the effects of a security incident or to protect a vulnerability.

Cybersecurity Expert System Modeling

- Cybersecurity Expert System Modeling involves creating specialized systems that mimic the decision-making capabilities of human cybersecurity experts. These systems integrate knowledge from cybersecurity experts into a formal framework that can reason, analyze, and make decisions to address security issues.
- The system is typically split into two subsystems, such as the inference engine and the knowledge base represented as security rules. The foundation of this cybersecurity expert framework is the knowledge base.
- User Interface: The user interface allows interaction with the expert system. It presents initial security facts or inputs to the inference engine and displays the results or decisions derived from applying the rules



Conclusion

Role of AI in Cybersecurity: AI methods like machine learning, deep learning, NLP, and expert systems are crucial for intelligent cybersecurity services.

Challenges in Data Collection: Gathering diverse, real-world cybersecurity data (structured, semi-structured, unstructured) poses significant challenges due to multiple sources and legal considerations.

Enhancing Security Models: Advanced analytics and improved machine learning techniques are needed to address issues like data sparsity, behavioral analysis, and optimizing security models.

Extracting Insights from Data: Effectively mining unstructured data using NLP and developing intelligent security models are critical research directions.

Rule-Based Systems: Developing lightweight, effective rule-based systems for cybersecurity, considering complexity and reasoning challenges, is essential.

Security Framework Design: Designing comprehensive cybersecurity frameworks that integrate AI-based advanced analytics to intelligently resolve security issues is pivotal.

Future Research Directions: Focus areas include refining AI techniques for cybersecurity, designing effective rule-based systems, and evaluating cybersecurity frameworks through rigorous experimentation.