LEVEL 0 SUMMARY TEMPLATE

Instruction

This summary will be shared with L1, L2 and L3. Keep in mind that these levels do not have a full understanding of the subject. Try to write something easy to understand but not simplistic. Your summary should explain the main contribution of the paper with your own words. Furthermore, you can use simple examples, if necessary, to better explain the main ideas. Your grade will take into account the quality of your summary, the formal English language in which it has been written, and whether it helps the levels above in their own work.

Name of student: Sanaa Dahour

Name of your Level 1: L0

Source (e.g. scholars.google.com): Google scholars

Paper title: Cyber Security Threat Intelligence using Data Mining Techniques and Artificial Intelligence

Keywords specific to the paper:

Summary of the main contributions:

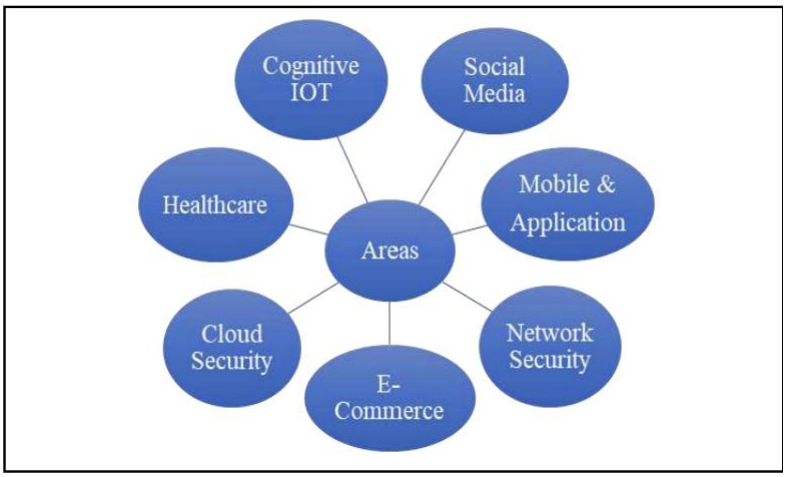
(Use text paragraphs, tables and if necessary, figures):

- AI model used (e.g. Neural network, etc.)
- Introduce the AI models
- How do they contribute the idea proposed by the paper?

Supported by a software application? (If yes, provide more details) NO.

Companies are as is well known more vulnerable to ongoing threats from cybercriminals who take advantage of holes in technology and associated processes. These attackers target all organizations whether they are in the public or private spheres. Cybersecurity uses algorithms procedures and defensive tools to deal with this problem. Preventing data corruption attacks and unauthorized access is the aim in safeguarding their most valuable information. Organizations must safeguard their most important information especially those that handle a lot of sensitive data. Reduced false positives and false negatives are the main goals of cybersecurity measures which target advanced common and emerging threats. Even with the widespread use of security measures like firewalls and antivirus software intrusions still happen on a regular basis. Sectors that necessitate strong threat detection include telecommunications credit card companies and commercial banks because they are particularly open to attacks. Among the most frequent threats are the unauthorized access to confidential information and the disruptive use of IT services by attackers. Because of the exponential growth in data generated there is an increasing need to strengthen cybersecurity against cyberattacks. Most of these attacks come as a surprise and are of great significance. Thus safeguarding the most important information about the company is the aim of cyber security.

CYBER SECURITY THREAT INTELLIGENCE USING DATA MINING TECHNIQUES AND ARTIFICIAL INTELLIGENCE



Talking about financial threats, by using correct IA and algorithms we can help protect and predict financial trends. The current analyzing techniques are not efficient for a large-scale implementation. As the amount of data is huge, and composed of structured and non-structured data, it makes the job more complicated to deal with. The organizations use tools based on sensors and intrusion detection techniques for network monitoring.

Various techniques and algorithms such as classification, clustering, prediction, fuzzy logic, artificial neural networks, support vector machines, and genetic algorithms are used in order to identify malicious users and anomalous patterns. Clustering actually helps understand patterns and perform statistical analysis based on similar attributes, while classification groups different cyberattacks together to detect threats. Prediction uses information learned from user behavior to predict hidden future attacks.

So, the document explores the domain of Cyber Security Threat Intelligence, focusing on the utilization of Data Mining Techniques and Artificial Intelligence. It underscores the significance of threat intelligence in detecting cyber-attacks, the application of artificial intelligence methods for identifying cyber threats, and the role of data mining in enhancing the accuracy of threat data in cybersecurity. The study advocates for the adoption of prominent artificial intelligence methods to pinpoint cyber-attacks and conduct data analysis to guide industries on incident response strategies.

Additionally, it explores diverse data mining approaches aimed at improving the accuracy of threat data in cybersecurity. The research also examines the challenges confronted by industries in safeguarding Internet-connected systems and the ethical considerations surrounding artificial intelligence algorithms in cybersecurity applications. The document emphasizes the necessity for dependable information security techniques and systems to effectively combat cyber threats, given the evolving nature of cyber-attacks and the growing reliance on Internet-connected devices across various sectors.