CHAPTER I
INTRODUCTION

1.1 Background

The rapid growth of technology in the digital era is distinguished by rising computational capacity to enable the data interchange process that happens. Data that was previously conventional in its exchange process is now digitized. However, the change in process makes it vulnerable to attack, especially cyber attack. Cyber attack is a form of effort carried out illegally to disrupt, damage, or gain access to certain documents or systems on computer networks, both personal and business (Microsoft, n.d.). As a matter of fact, according to CNBC INDONESIA, Microsoft discovered a cyber threat launched by a Chinese hacker group, Typhoon, against vital communications infrastructure between the US and Asia with the aim of obtaining intelligence information (Sorongan, 2023). This threat also impacts an institution, organization or country with the consequences of these attacks being severe, including damage to reputation, financial loss, and potentially harm to individuals or the wider community.

Cyber threats launched by attackers certainly do not solely attack a country without a specific target. Threats that often occur can be divided into 3 (three) parts, Specifically, risks generated by hardware inadequacies, software-based bugs, and vulnerabilities in computer internet networks (Aslan. Ö, 2023). Cyber threats that attack computer internet networks continue to increase every year and have had a significant impact beyond the companies involved. These threats can be carried out in various ways such as malware infections, Denial-of-Services (DoS), phishing, data breaches, and insider threats. This threat certainly provides losses such as in the United States region. Based on data provided by Kindness Financial Planning

(Appel, 2022) that there are 10 regions in the United States that have suffered losses from cyber-attacks as shown in figure 1.1.

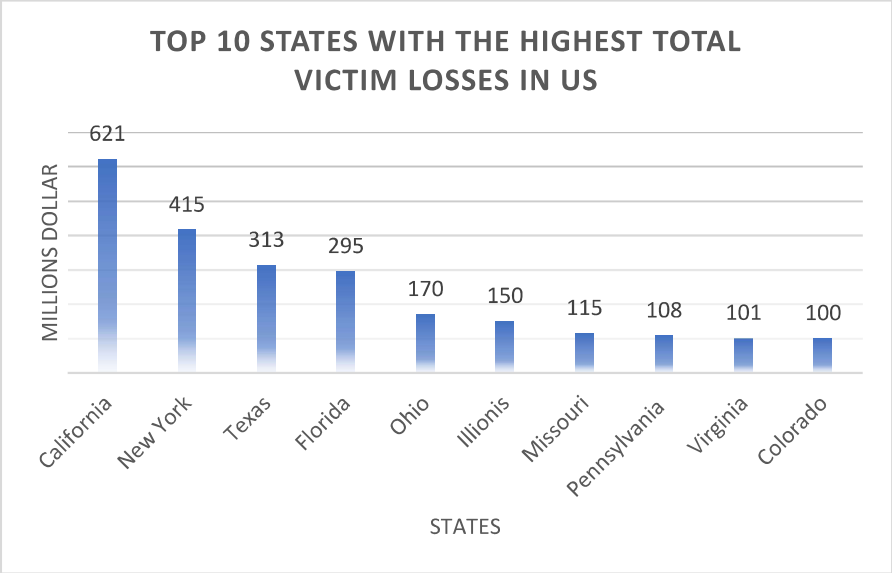

Figure 1.1 Top 10 States with the Highest Total Victim Losses in US

Source: (Appel, 2022)

SolarWinds, an IT firm based in Austin, Texas, United States, provided an IT performance management and monitoring system called Orion in 2020. Orion has access to clients' system performance logs and data, making it a potential target for hackers. The platform was compromised, affecting thousands of systems and clients on a global level. Hackers then used a supply chain attack to insert a malicious virus called a remote access trojan (RAT) into the Orion framework. In this case, more than 18,000 systems worldwide were infected with the virus and caused billions of dollars in irreparable damage (Jena, 2023). From the case that happened to SolarWinds, it can be said that a computer internet network system can be carried out dangerous threats that certainly cause great losses and reduce the reputation of a company. With this threat, a country needs to have cybersecurity to protect its crucial points.

Cybersecurity is a form of activity to protect networks, computers, software applications, data, and critical systems from potential digital threats (Amazon Web Services, n.d.). In the context of national defense, cybersecurity can be carried out by continuing to monitor or safeguard public interests from all forms of disturbances, particularly in the sphere of critical information infrastructure in Indonesia. This is reinforced by the issuance of Presidential Regulation (Perpres) Number 82 of 2022 concerning Critical Information Infrastructure (CII) by President Joko Widodo (Biro Hukum dan Komunikasi Publik BSSN, 2021). Disruptions to Critical Information Infrastructure (CII) can cause very serious losses and impacts on the public interest, defense and security, public servants, and the national economy.

Disruptions to Critical Information Infrastructure (CII) that result in severe losses and consequences may undoubtedly be examined to reduce large losses for a government. The process of studying the computer internet network system can be accomplished by identifying attacks on the internet network. If these are detected, the type of assault can be determined. Network traffic is recorded, stored, and analyzed immediately, and incident response is triggered (Pilli. E. S, 2010). Network traffic is certainly an important reference in the analysis process. Network anomalies are network traffic that is odd and sudden, and occurs in a short period of time from normal network traffic (Ahmed. T, 2007). Detecting attacks involving failed devices on the network, network strain flash crowding, worms, port scanning, unsafe inside user activity, fraudulently spread Denial of Service (D-DoS) attacks, network intrusions, and so on that interfere with normal network service delivery is currently a critical issue (Rahme. S, 2009). With the attack that occur, it is necessary to have network monitoring that is appropriate and efficient in the process. Network monitoring

methods are of course tailored to the needs, understanding, and adequate attributes.

Network monitoring must be adjusted to increase the process's time efficiency. Deep learning can be used to modify the monitoring approach. Deep learning is one of several machine learning approaches. Learning is built on the concept of extracting features from raw data by applying many layers to identify various aspects relevant to the input data. Deep learning techniques include convolutional networks, artificial neural networks, and deep neural networks (Mishra. R. K, 2021). Among the several known methodologies, researchers picked the Deep Belief Network method for this investigation. Deep Belief Network is a method that uses a stack of Restricted Boltzmann Machines (RBM) or autoencoders (Dr. SULARTOPO S.Pd., 2021). In his paper titled "Using Deep Learning Model for Network Scanning Detection" (Viet. H. V, 2018), he presents the results of his experiments with network scanning and deep belief network techniques using a combination of supervised and unsupervised methods. Experiments utilizing the NSL-KDD dataset and the UNSW-NB15 dataset reveal that the deep belief network method has a high value for detection in network scanning.

Based on the above background, security on computer internet networks, especially on Critical Information Infrastructure (CII) is needed due to the many criminals who threaten networks using dangerous viruses for important data security. Therefore, researcher will modify the method, especially the deep belief network method combined with Isolation Forest as a form of monitoring computer internet networks. This modification is to produce an analysis related to the deep belief network method combined with the isolation forest method which is compared with the deep belief network combined with the support vector machine method, where the combination results in

an evaluation of internet network attack detection aimed at strengthening cyber security. Researcher hope that in the process of modifying this method, it will be able to monitor network attack that occur efficiently and provide insight and contribution in the future. Also, for future work to be done consider technology or hazard changes that might impact the efficacy of your model.

1.2 Problem Identification

From the background outlined earlier, problem identification is found from this research. The author writes that the problem identification obtained is as follows:

a. Despite the issuance of the Presidential Regulation on the Protection of Critical Information Infrastructure (CII), there is no maximum implementation and law enforcement to maintain the security and integrity of the country's important data and information from cyber-attacks and threats.
b. Cyber threats often occur due to weak security levels and lack of efficiency and accuracy in detecting attack on the internet network.

1.3 Problem Limitation

So that the discussion in this study does not deviate, the authors provide a limitation on the scope of the research. The scope given in this study includes:

a. The dataset used in this study uses existing datasets on network attack, KDDCUP ‘99.
b. Programming using Python programming language.
c. The method using Deep Belief Network, Isolation Forest, and Support Vector Machine method.

1.4 Problem Statement

Based on the background of the existing problems, we can formulate the problems that occur:

a. The design and implementation of the DBN model need to be researched further to see how this model can support cybersecurity.
b. Utilizing Deep Belief Network methods to improve efficiency and accuracy in detecting attack can potentially reduce weaknesses.

1.5 Research Objectives

Based on the existing background, the objectives of this study are:

a. Create a model that is able to detect attack in computer internet networks using the Deep Belief Network, Isolation Forest, and Support Vector machine methods.
b. Evaluate the performance of the designed system to ensure that the methods used are effective in detecting attack.

1.6 Research Benefits

Based on the above background, researchers found theoretical and practical benefits. Theoretical benefits are benefits in the context of understanding cyber attack, namely:

a. Assist in deepening the understanding of the increasingly complex and increasing cyber threats.
b. Provide understanding in identifying and classifying the types of threats that may occur.
c. Provide more insight into how cyber threats can affect Critical Information Infrastructure and affect reputation, especially the country's reputation in cybersecurity.

Then the practical benefits are benefits that provide solutions in the context of more effective cybersecurity to protect Critical Information Infrastructure, especially in internet network security. Among them are:

a. The modified deep belief network method combined with the isolation Forest method can help in network attack detection. It can identify potential attacks or disturbances on the network more efficiently.
b. This research reinforces the importance of complying with applicable regulations, one of which is Presidential Regulation No. 82 of 2022 in order to maintain the security of Critical Information Infrastructure and other critical infrastructures.