CHAPTER II
LITERATURE REVIEW

2.1 Theoretical Foundation

2.1.1 National Defense

National defense is the protection and safeguarding of a country's sovereignty, territorial integrity, and citizens' well-being against external threats. It entails a comprehensive set of policies, strategies, and military capabilities designed to discourage potential aggressors and effectively respond to any kind of aggression or attack. According to the Regulation of the Minister of Defense No. 16/2012 According to the Policy of Integration of State Defense Components, national defense encompasses all efforts to protect the sovereignty of the state, the territorial integrity of the Unitary State of the Republic of Indonesia, and the overall safety of the nation. The national defense effort takes into account the dynamics of the many types of threats encountered. The variety of threats, both military and non-military, is always changing as the strategic environment evolves. State defense functions to realize and preserve the entire territory of the Unitary State of the Republic of Indonesia as a defensive unit. State defense is planned and outfitted early with a state defense system by building up the capabilities and deterrents of the state and nation, as well as overcoming any threats.

National defense today goes beyond traditional military strategy to include cyberspace. Cyber national defense, in the context of protecting a country's sovereignty and residents' well-being, is critical in the face of rising technological threats. It entails safeguarding not just physical borders but also digital frontiers from cyber threats that have the potential to jeopardize key infrastructure, sensitive information, and national security. The Minister of Defense's

Regulation No. 16/2012 emphasizes the policy of integrating state defense components and highlights the integration of cyber capabilities into national security strategies. In this context, cyber national defense refers to any actions aimed at preserving the state's sovereignty and territorial integrity, as well as safeguarding the protection of its citizens in the digital domain. The notion of cyber national defense entails organizing and planning the government's reaction to cyber threats by establishing a strong state defense system. This system focuses on developing and enhancing the cyber capabilities required for early detection, prevention, and response to cybersecurity threats. Cyber national defense also underlines the need for a cyber deterrence plan to discourage possible enemies from engaging in destructive cyber actions. The purpose of cyber national defense is to keep the entire national territory as a defensive unit, not just in physical terms but also in cyberspace. To keep ahead of evolving cyber dangers, we must continue to invest in cybersecurity technologies, qualified individuals, and collaborate with foreign partners.

2.1.2 Critical Information Infrastructure (CII)

Critical Information Infrastructure (CII) is an important part of a country. CII concerns every organization or sphere of government that is crucial for the progress and development of the country. CII itself can be defined as an electronic system whose entire process utilizes information technology or operational technology that runs independently or is interconnected with other electronic systems that support the strategic sector (Biro Hukum dan Komunikasi Publik BSSN, 2021). The term CII is the approval of KEPPRES No. 63 of 2004 regarding the protection of national vital objects, which specifies that areas/locations, buildings/installations, and/or businesses that impact the well-being of many individuals, national security, and/or

strategic ways to earn state revenue; and PERPRES No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, which states that an electronic system is a series of electronic devices and procedures that function to pr Aside from that, electronic transactions are legal activities carried out using computers, computer networks, and/or other electronic means.

CII itself has sectors that have been determined in PERPRES No. 82 of 2022 concerning the Protection of Critical Infrastructure Information as strategic and crucial sectors, including Government Administration, Energy and Mineral Resources, Transportation, Finance, Health, Information and Communication Technology, Food, and Defense. The strategic sectors stipulated in PERPRES No. 82 of 2022 concerning the Protection of Critical Infrastructure Information are certainly the target of cyber-crime. CII which refers to a system, network, software, or data that is confidential for the operational continuity of an organization, institution, or country, makes it an important or crucial element where information and communication play an important role in the life sector and the development of the country. Protection of these sectors is a must because data security and confidentiality are a form of integrity that is displayed, so that it can have a positive impact, namely public trust in organizations, institutions, and the state. In this research, the CII in question leads to the defense sector.

2.1.3 Cybersecurity

The usage of information and communication technology (ICT) in Indonesia, in particular, is growing rapidly. This use is, of course, directly proportional to the times and technical advancement. In fact, the use of information and communication technology has permeated every part of life, such as social, economic, and bigger aspects such as international collaboration. This digital evolution has given birth to

the concept of cyberspace, which is where these activities take place. However, with this potential come enormous concerns, the most prominent of which is cybersecurity. Cybersecurity ontology is essential to properly address these issues which can be defined with a shared knowledge model to standardize security terminologies, organize the relationships between them, and eliminate semantic differences between different security policies in the IoE (Xue. X, 2022). In the Indonesian context, this ontology provides a formal framework for understanding, specifying, and controlling cybersecurity. It categorizes cyber hazards, provides security measures, emphasizes regulatory compliance, and encourages stakeholder collaboration. Furthermore, the ontology teaches individuals and organizations about the significance of cybersecurity while also ensuring effective incident response and data privacy protections.

According to Minister of Defense Regulation No.82 of 2014 concerning Cyber Defense, cybersecurity can be defined as a form of effort in the form of maintaining the integrity, confidentiality, and availability of information and all supporting facilities that are cross-sectoral in nature. In addition, cybersecurity can be said to be a protection to protect devices and services connected to the internet from malicious attacks from hackers, spammers, and cybercriminals (Kelley, 2023). However, according to Craigen (Craigen. D, 2014) in his publication, which did a literature review on cybersecurity, is the group's and collecting of elements, procedures, and mechanisms used to defend cyberspace and its supporting systems from occurrences that lead to de jure and de facto property rights to change.

From the book that written by Daniel Shoemaker (Shoemaker. D, 2020) there are eight cybersecurity body of knowledge (CyBOK). CyBOK can be defined as a thorough and systematic reference aimed

at defining and organizing the key knowledge areas and concepts in the field of cybersecurity. It is intended to serve as a starting point for cybersecurity professionals, researchers, educators, and policymakers. But this research is focus in data security knowledge area, especially in secure communication protocol. This knowledge talked about the implications of network protocols and network security for securing data security. Daniel also talked that there are five areas that relevant in this knowledge area, these are Application and Transport Level Protocols, Attacks on TLS, Internet Network Layer, Privacy Preserving Protocols, and Data Link Layer that can you see in figure 2.1.

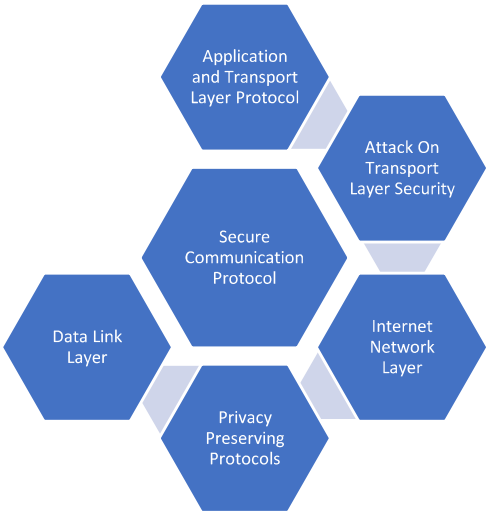

Figure 2. 1 The secure communication protocols knowledge unit topics.

Source: (Shoemaker. D, 2020)

Cybersecurity is certainly needed to anticipate the arrival of a threat or attack so that it requires readiness and responsiveness in dealing with it and being able to restore the situation due to the impact of the threat or attack. According to the National Cyber Security Index (NCSI), Indonesia ranks 49th in the world in terms of cybersecurity.

This data shows that Indonesia still has to improve its cybersecurity quality in order to maintain CII which is very influential on the development and progress of Indonesia. Even this ranking is still below Malaysia (22nd), Singapore (31st), and Thailand (45th) in cybersecurity aspects around the world (NCSI, n.d.). However, Indonesia's ranking has continued to improve since 2019 which was 103rd although it had dropped to 110th in mid-2020 but Indonesia continued to improve until it was 49th in 2023.

2.1.4 Cyber Attack

Cyber attack is one of the challenges of today's technological world. According to PERMENHAN No.82 of 2014 concerning Cyber Defense, cyber threat is a form of desire to carry out illegal violation activities and violate laws, norms, or information security with the aim of obtaining material and immaterial benefits. This threat can be carried out by state actors or non-state actors. Therefore, the threat can be individual, group, group, organization, or a country.

Cyber threats undoubtedly have characteristics that lie beneath the threat. These factors can include ideological, political, economic, social, cultural, and other factors that motivate people to commit cybercrime. Cyber threats in the context of threats in Infrastructure Information Vital can be separated into three primary categories in order to achieve the goals of these aspects. The first is malware threats, which are malicious software in the form of viruses, worms, trojans, ransoms, and spyware. This malware threat can steal, damage, or disrupt an operating system or network. The second threat is DoS and DDoS (Distributed Denial-of-Services) attacks, which are forms of threats that aim to impede the flow of network traffic by sending fake traffic to a system or server continuously. The third threat is hacking, which is an unauthorized attempt to enter a system or network with the aim of damaging or stealing data.

2.1.5 Defense Science

Defense can be interpreted as an effort or strategy to protect oneself, as well as the country from a threat which can later be used as a major instrument to create national security (Mardhani. D, 2020). Referring to the context of creating national security, especially in Indonesia, Indonesia issued regulations in the Constitutional Law of the Republic of Indonesia No. 3 of 2002 concerning State Defense, paragraph one of article one states that national defense refers to initiatives to protect the supremacy of the country, the borders of the Unitary Republic of Indonesia, and the safety of the entire country from threats and disruptions to the trustworthiness of the nation and state.

According to the Regulation of the Minister of Defense of the Republic of Indonesia Number 82 of 2014, cyber defense can be defined as an endeavor to overcome cyber threats or attacks that may disrupt the process of implementing national defense. This is to foresee the coming of a cyber threat and attack, so that readiness is required in dealing with cyber threats and attacks, which can later be restored by responding to the repercussions of the cyber threat or assault.

2.1.6 Deep Belief Network

Deep Belief Network is a graph-based deep learning model. It is very useful for unsupervised learning and representation of feature extractions from unlabelled databases (Bello. R. W, 2021). In a journal written by Ira Zulfa, Deep Belief Network (DBN) is a Deep Learning advancement in the form of a stack of multiple algorithms or approaches that have the objective of feature extraction that maximizes the use of all resources (Zulfa. I, 2017), in which each layer of hidden variables captures the higher-order correlation between the activity of the hidden features and the lower layers (Salakhutdinov. R,

2008). DBN can also create a neural network including hidden neural layers. Furthermore, data representation is extremely crucial in machine learning. As a result, numerous techniques for feature extraction, learning, and preprocessing have been developed (Keyvanrad. M. A, 2014).

DBN's architecture combines unsupervised learning techniques with neural networks. The architecture is composed of layers of Restricted Boltzmann Machines (RBM) that are trained one at a time in an unsupervised way (Tabrez, 2023). Every RBM in the DBN is trained independently by employing contrastive divergence, an unsupervised learning technique. This method can estimate the gradient of the data's log-likelihood for RBM parameters. The output of one trained RBM is then used as input for the following RBM, which is done by stacking the trained RBMs on top of each other. Once the DBN is trained, supervised learning tasks can be performed by adjusting the final layer weights using supervised learning techniques such as backpropagation. This refinement process can improve the performance of the DBN on the specific task being trained.

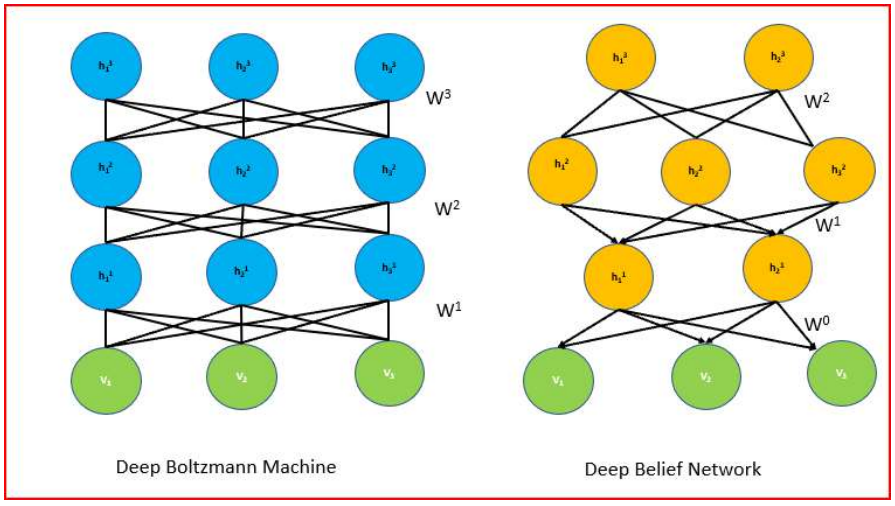

Figure 2. 2 The Architecture of DBN.

Source: (Kalita, 2022)

2.1.7 Isolation Forest

The isolation forest method is similar to the random forest method, which employs an ensemble of binary trees. The random forest method improves classification/regression accuracy by creating an ensemble of binary trees and enabling them to select the most popular or often occurring class or regression (Chen. Y, 2018). However, isolation forest differs from random forest. The isolation forest detects attacks by growing the ensemble of binary trees and calculating the level of attack by calculating the distances taken from each ensemble of trees and generating an ongoing randomized rotation process of a sample picked from the sample population (Liu, 2008).

During tree construction, nodes conduct separate by randomly dividing with a random feature and deciding on quantities amongst the highest and lowest values (Liu, 2008). To demonstrate the isolation trees process, a binary tree structure with nodes and edges can be used to display the isolation of six unique unit cells. An isolation tree node may serve as an exterior node without any children or an interior node with just one test and two child nodes (Liu, 2008).

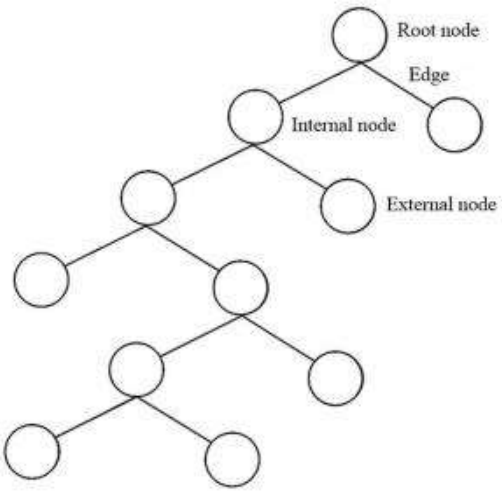

Figure 2. 3 Diagram of an isolation tree for randomly partitioning six unique unit cells.

Source: (Liu, 2008)

2.1.8 Support Vector Machine

Support vector machines (SVMs) are highly effective machine learning approaches for data classification and pattern identification. Vapnik created SVMs based on statistical learning theory (Zhang. Y, 2013). The primary principle of SVM is to translate the input vectors to a feature with a high dimension space and build a linear decision surface in that space (Cortes. C, 2004). This allows SVMs to perform nonlinear classification in the original input space. SVM can achieve high generalization performance even when the training data is limited.

SVM has been applied to many domains, including fault diagnosis of coal mining equipment optical character recognition (Cortes. C, 2004), and network traffic classification. SVMs have been shown to outperform other machine learning techniques such as artificial neural networks in several applications. SVM training involves

solving a convex quadratic programming problem to find the optimal separating hyperplane between classes. This can be done using various algorithms, including the Lagrangian SVM algorithm. SVMs can also be extended to handle non-separable data by using slack variables and kernel functions.

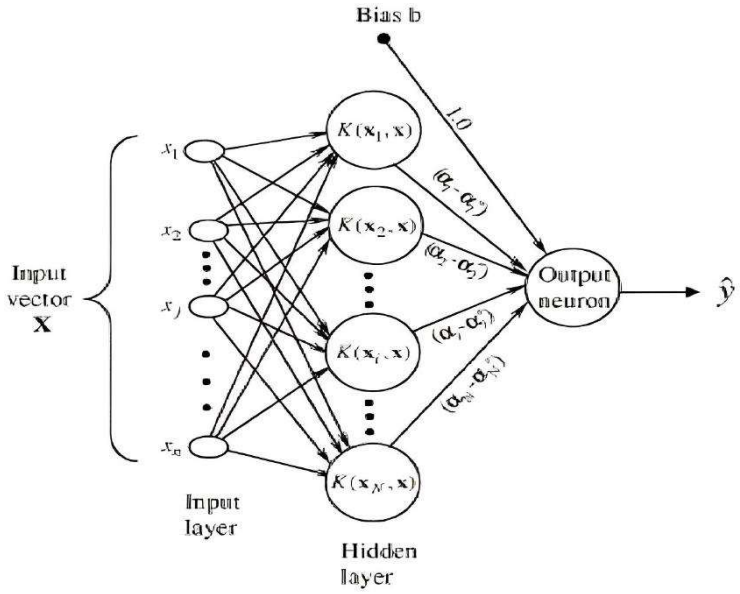

Figure 2. 4 Architecture of support vector machine

Source: (Farid. N, 2013)

2.2 Previous Research

In the writing topic chosen, the author certainly looks for references to previous research as the basis for this research. The selected previous research is adjusted to linearity in the scope of research, especially in the deep belief network method. This reference is used as a reference for the research that the author examines, as the scope of finding the appropriate research gap, so that researchers can develop this method. The table below shows previous research which contains information in the form of the author's name, research title, similarities in research, and the results of previous research.

Table 2. 1 Previous Research

No.	Researcher Name	Research Title	Method	Result
1.	(Manimurugan. S, 2020)	“Effective Attack Detection in Internet of Medical Things Smart Environment Using a Deep Belief Neural Network”	Using Deep Belief Network in their experiment	The DBN result method for DDoS Attack Detection shown: Accuracy: 96.67% Precision: 95.21% Recall: 97.34% F1-Score: 0.97 Detection Rate: 97.31%
2.	(Malik. R, 2022)	“An Improved Deep Belief Network IDS on IoT-Based Network for Traffic Systems”	The paper uses DBN (Deep Believe Network) in their experiment for IDS on IoT-Based Network for Traffic Systems	The result DBN using TON_IOT_Weather sample dataset: Precision: 0.78 Recall: 0.90 F1-Score: 0.84 Accuracy: 86.3
3.	(Balakrishnan. N, 2019)	“Deep Belief Network Enhanced Intrusion Detection System to Prevent Security Breach in the Internet of Things”	The paper uses DBN (Deep Belief Network) in their experiment for an improved Intrusion Detection System to avoid breaches of security	The IDS-DBN outperformed the DGA's F1 Score in identifying DoS, Overflow, SSH Brute Force Login, Suspicious DNS queries, and Cache Poisoning attempts

No.	Researcher Name	Research Title	Method	Result
				Malware infection above 0,95
4.	(Thanh, 2020)	"A Novel Approach for Intrusion Detection Based on Deep Belief Network"	Using Deep Belief Network in their experiment	The DBN result method for Attack Detection in accuracy shown: 99.16%
5.	(Yang. Y, 2018)	"Building an Effective Intrusion Detection System Using the Modified Density Peak Clustering Algorithm and Deep Belief Networks"	The paper using DBN (Deep Believe Network) in their experiment for Building an Effective Intrusion Detection System	The technique that purpose with MDPCA-DBN for each dataset shown: 1. NSL-KDD (KDDTest+) Accuracy: 82.08 DR: 70.51 FPR: 2.62 2. NSL-KDD (KDDTest-21) Accuracy: 66.18 DR: 61.57 FPR: 13.06 3. UNSW-NB15 Accuracy: 90.21 DR: 96.22 FPR: 17.15
6.	(Viet. H. N, 2018)	"Using Deep Learning Model for Network Scanning	The paper uses DBN (Deep Belief Network) in their	Result of TPR and FAR-NSL-KDD, DBN has the highest score

No.	Researcher Name	Research Title	Method	Result
		Detection"	experiment for network scanning	in **0,99458** compare with ANN-MLP, AOCD, and SVM as the lowest score. Get the highest score in accuracy in **99,64** for detect ipsweep, nmap, port sweep, and satan attack.
7.	(Chen. J, 2023)	"An Anomaly Detection Method for Wireless Sensor Networks Based on the Improved Isolation Forest"	The research uses isolation forest, but this study proposes BS-iForest and then evaluates the results using AUC (Area Under Cover).	The AUCs on the BreastW dataset reached 0.9947 and on the campus CRS dataset reached 0.989.
8.	(Tao. X, 2018)	"A parallel algorithm for network traffic anomaly detection based on Isolation Forest"	In order to discover network anomalies, the authors suggest a parallel approach based on Isolation Forest.	The result on AUC and accuracy with the experiment of the researcher propose: 1. IForest AUC: 0.8831 Accuracy: 86.872 2. SPIF AUC: 0.8927 Accuracy: 87.144

No.	Researcher Name	Research Title	Method	Result
9.	(Sudha. M. S, 2021)	"An optimized deep belief network to detect anomalous behavior in social media"	The Deep Belief Network Interactive Autodidactic School (DBN-IAS) algorithm is developed for detecting anomalies in social networks.	the detection rate is 99.32%
10.	(Li. C, 2021)	"Similarity-Measured Isolation Forest: Anomaly Detection Method for Machine Monitoring Data"	The similarity-measured isolation forest (SM-iForest) is proposed for detecting aberrant segments and their associated data. The inadaptability and instability of iForest were minimized while processing MMD benefiting from the properties of sliding-window processing. Furthermore, an anomaly identification stage	The model of this research found that the Similarity-Measured Isolation Forest detect: • Detection Rate: 100% • False Alarm Rate: 9.20%

No.	Researcher Name	Research Title	Method	Result
			that measures the relative similarity of possible anomalous segments increased iForest's robustness	
Positioning				
11.	Researcher	Comparison Analysis with Deep Belief Network Model to Detect Network Anomalies for Strengthening Cybersecurity in Data Center	The research uses DBN (Deep Belief Network) combain with isolation forest also combain with support vector machine	The result on this positioning is: 1. DBN AUC: 0.92 Accuracy: 0.93 Precision Normal: 0.98 Attack: 0.77 Recall: 0.91 F1-Score:0.83 2. DBN and IForest AUC: 0.92 Accuracy: 0.93 Precision Normal: 0.99 Attack: 0.60 Recall: 0.95 F1-Score: 0.72 3. DBN and SVM AUC: 0.91

No.	Researcher Name	Research Title	Method	Result
				Accuracy: 0.92 Precision: Normal: 0.95 Attack: 0.60 Recall: 0.92 F1-Score: 0.72

The analysis of the presented research studies unveils a comprehensive exploration of diverse applications and methodologies within the cybersecurity domain. Manimurugan (2020) notably demonstrated the efficacy of Deep Belief Network (DBN) in securing the Internet of Medical Things (IoMT), achieving high accuracy and robust DDoS attack detection. Rayeesa Malik (2022) extended the capabilities of DBN for an enhanced Intrusion Detection System (IDS) in IoT traffic, showcasing commendable precision, recall, and accuracy. Furthering the scope of DBN in IoT security, Nagaraj Balakrishnan's study (2019) achieved F1 Scores exceeding 0.95 for various security threats. Thanh's innovative DBN-based approach (2020) showcased remarkable accuracy in intrusion detection. Yanqing Yang (2018) introduced MDPCA-DBN for effective intrusion detection, revealing varying accuracies across datasets.

Additionally, Hung Nguyen Viet's study (2018) employed DBN for network scanning detection, surpassing other models with the highest accuracy. Studies incorporating Isolation Forest, such as Chen's (2023) BS-iForest and Xiaoling Tao's (2018) parallel approach, demonstrated competitive anomaly detection capabilities. The proposed models, including SM-iForest by Changgen Li (2021), exhibited high detection rates for abnormal segments in machine

monitoring data. The research positioning comparison, integrating DBN with Isolation Forest and SVM, adds a crucial layer to the analysis by elucidating trade-offs in precision, recall, and F1-Score for each combination. This research significantly contributes valuable insights into the effectiveness of hybrid models for detecting network attack within the context of cybersecurity.

2.3 Thinking Framework

A thinking framework is a structured approach to problem solving that assists people and teams in navigating complex challenges and developing unique solutions. It is a method of structuring thoughts and activities so that challenges can be understood and approached from different angles (Johnson, 2014). Thinking framework give a benefit for doing research, there are:

a. Clarity

   Framework thinkers can provide clarity in situations. Good frameworks focus everyone's thoughts, allowing the team to tune out the noise and focus on the most important questions.

b. Progress

   Frameworks can help to break down barriers and speed up the process of finding solutions. The capacity to make decisions quickly can mean the difference between success and failure.

In this research, researcher try to pour the thinking framework about this research that can be seen in figure 2.5. The figure shows a diagram that illustrates the process of using the DBN model to detect network attack. The problem mentioned in this research is that cyber threats continue to arise on the internet network, making cyber security critical. However, while cyber security on the internet network is still weak, cyber security has become an important feature, so the

Indonesian government issued Presidential Regulation (Perpres) Number 82 of 2022 concerning Protection of Critical Information Infrastructure (CII) in an effort to improve cyber security. Therefore, researchers implemented a study to design a DBN model for identifying network attack. A previous explanation follows as input in research, which follows up by network data collected from the KDDCUP '99 dataset.

The following stage is process, which is a network data processing process utilizing the DBN paradigm. DBN is a form of artificial neural network made up of multiple layers. These layers are linked together to build a complicated network, which can be used to investigate complex data patterns. The process stage is derived from the problem description in this research. So that it may analyze the DBN model and detect network irregularities caused by cyber threats.

After through a series of stages, the procedure produces an analysis of the Deep Belief Network (DBN) model. The model is then evaluated, particularly when combined with Isolation Forest and Support Vector Machine (SVM). The goal of this review is to assess how well these models enable cybersecurity. The analysis of the DBN model's results will shed light on the model's ability to detect network attack that could indicate cyber risks.

The performance of these two integrated models will be evaluated in order to discover their respective strengths and limitations. The investigation is expected to provide a more complete understanding of how integrating DBN with Isolation Forest and DBN with SVM can successfully increase cyber threat detection and response capabilities. The results of this review are likely to give significant suggestions for future development in increasing cybersecurity.

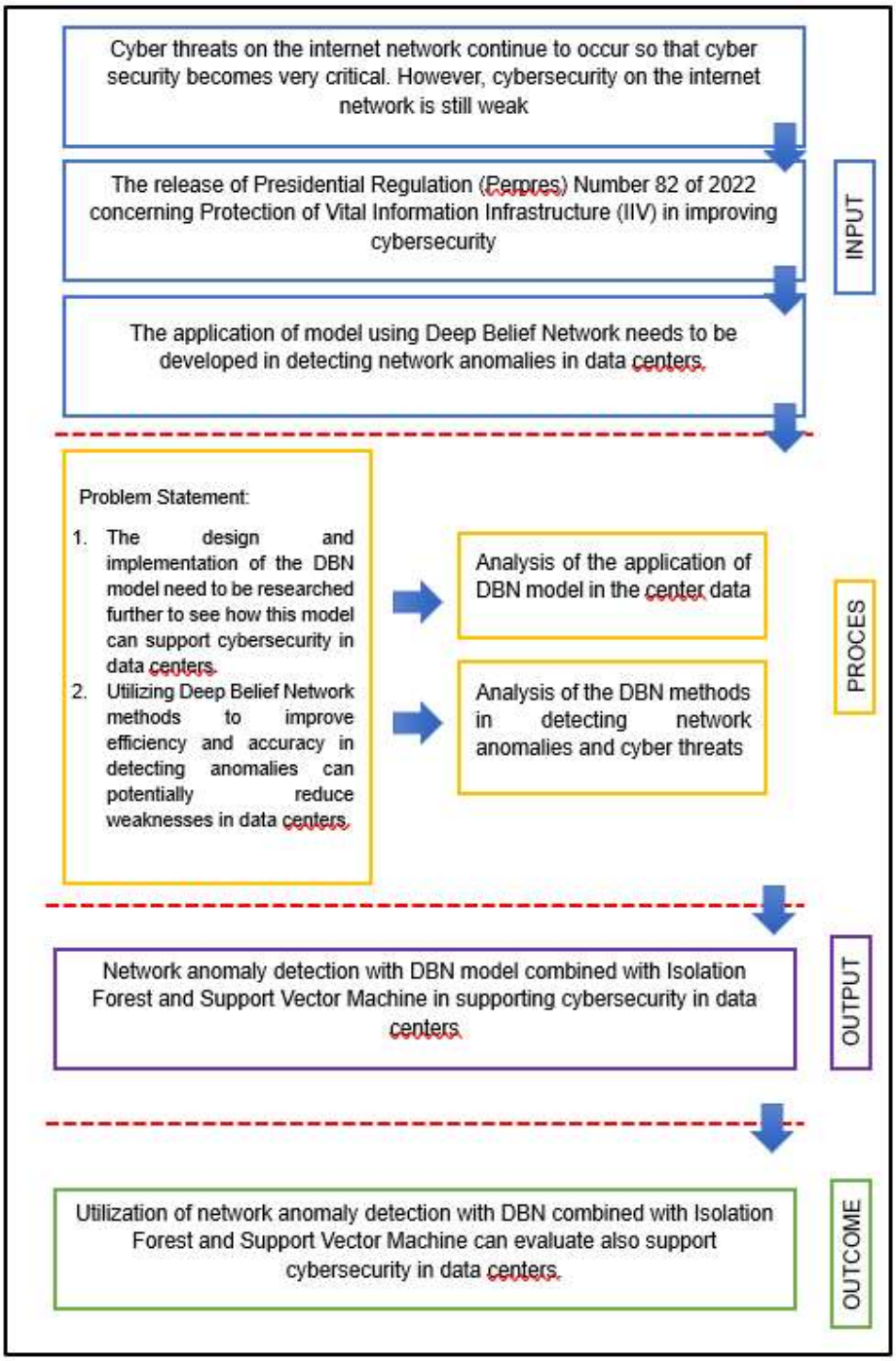

Figure 2. 5 Research Framework.