electronics

MDPI

Review

The Current Research Status of AI-Based Network Security Situational Awareness

Maoli Wang *, Guangxue Song, Yang Yu and Bowen Zhang

School of Cyber Science and Engineering, Qufu Normal University, Qufu 273165, China; sgx_1117@163.com (G.S.); yy_goahead@163.com (Y.Y.); zhangbwqfnu@163.com (B.Z.)
* Correspondence: wangml@qfnu.edu.cn

Abstract: Network security situational awareness is based on the extraction and analysis of big data, and by understanding these data to evaluate the current network security status and predict future development trends, provide feedback to decision-makers to make corresponding countermeasures, and achieve security protection for the network environment. This article focuses on artificial intelligence, summarizes the related definitions and classic models of network security situational awareness, and provides an overview of artificial intelligence. Starting from the method of machine learning, it specifically introduces the research status of neural-network-based network security situational awareness and summarizes the research work in recent years. Finally, the future development trends of network security situational awareness are summarized, and its prospects.

Keywords: artificial intelligence; machine learning; network security; neural network; situational awareness

Citation: Wang, M.; Song, G.; Yu, Y.; Zhang, B. The Current Research Status of AI-Based Network Security Situational Awareness. *Electronics* **2023**, *12*, 2309. https://doi.org/10.3390/electronics12102309

Academic Editor: Seokjoo Shin

Received: 27 April 2023
Revised: 17 May 2023
Accepted: 18 May 2023
Published: 19 May 2023

1. Introduction

According to the 50th Statistical Report on Internet Development in China released by the China Internet Network Information Center (CNNIC), as of June 2022, the number of Internet users in China has reached 1.051 billion, and the penetration rate of Internet applications has exceeded 74.4%. This development achievement has resulted in a significant impact on the history of human society, promoted economic and social development, and enriched people's ways of life. At the same time, it has also brought new security risks and challenges to network security.

In recent years, serious network security incidents have occurred frequently in China, and security threats and risks have become increasingly prominent. On 22 June 2022, Northwestern Polytechnical University issued a notice stating that the school's email management system had been attacked by network hackers, which posed significant risks to the school's teaching and campus life. As the cost of intrusion by network attackers continues to decrease and attack methods become increasingly advanced, the network security situation faced by critical information infrastructure is becoming increasingly severe, posing a serious threat to national security. At the same time, network attacks are becoming more complex and diversified, and traditional network defense methods are no longer sufficient to maintain network security. Therefore, situational awareness has become the key to future national network security. In a large-scale Internet environment, by searching, analyzing, and displaying various security elements that affect the Internet, we can better predict future Internet development trends. Among them, machine learning, as a major technical component of artificial intelligence, is mainly used in network security situational awareness systems by collecting a large number of data sets to establish training sets and then building machine-learning models to detect malicious traffic on the Internet in real time, thereby improving the efficiency and accuracy of the Internet.

This paper mainly summarizes and organizes the basic concepts of Internet situational awareness, system modeling, and the current research status of machine-learning-based

network security situational awareness, providing a reference for researchers in the field of network security; the structure of the article is shown in Figure 1. The contributions of this paper are as follows:

(1) Summarize the relevant concepts of network security situational awareness and organize relatively classic network security situational awareness models.
(2) Systematically overview the content of artificial intelligence and analyze in detail the current research status of network security situational awareness based on neural networks; and also summarize the specific implementation and application of network security situational awareness.
(3) Summarize the current research status of network security situational awareness and provide prospects for future development trends.

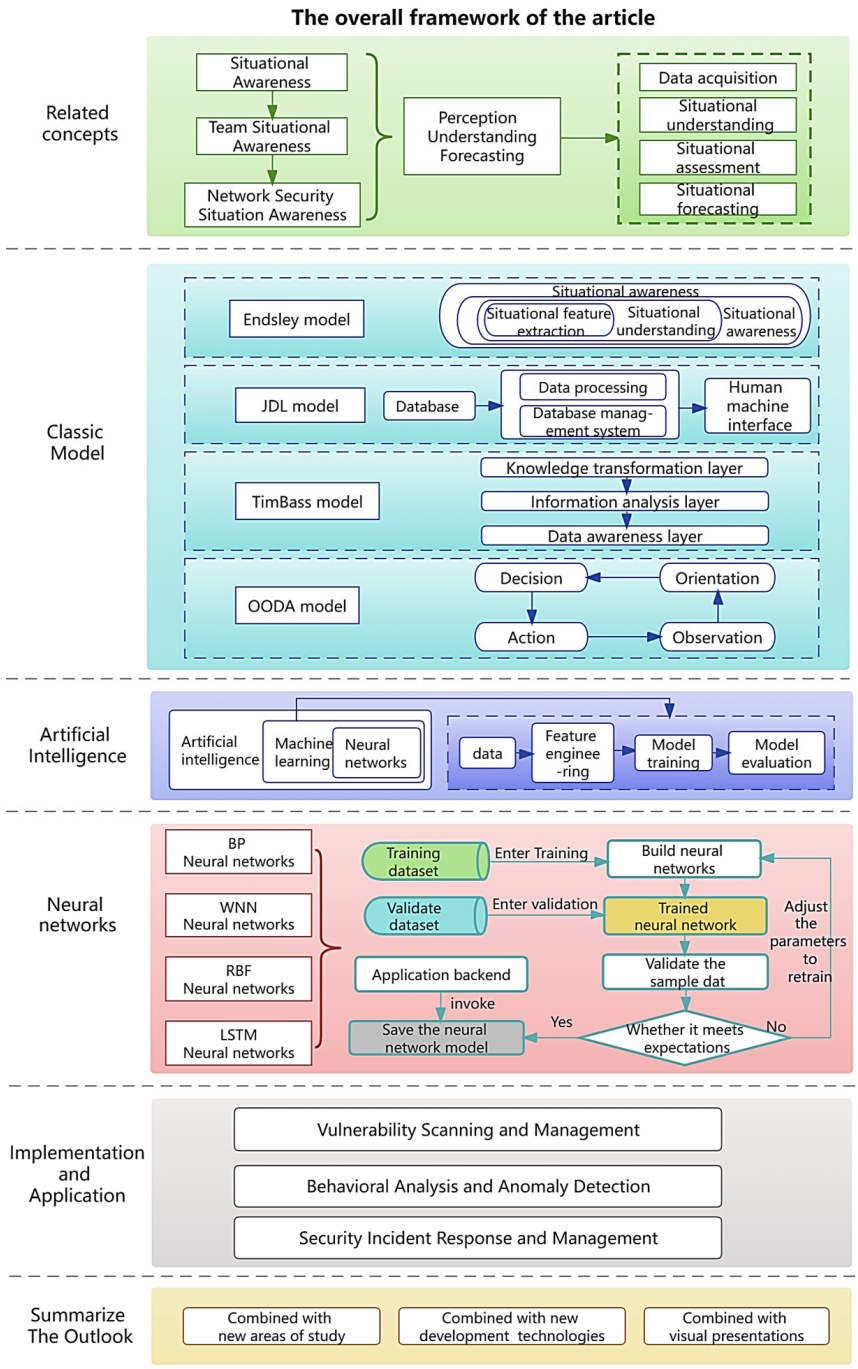

Figure 1. The overall framework of the article.

2. Related Concepts of Network Security Situational Awareness

The initial research on network security situational awareness can be traced back to the research based on intrusion detection systems (IDS). Early IDS mainly focused on detecting and defending against specific attack methods and features, but this method was vulnerable to attackers bypassing and deceiving the system [1–3]. Therefore, people began to study how to extract useful information from large-scale network traffic to more comprehensively and accurately understand the security status of the network, which is the foundation of network security situational awareness. However, with the continuous increase in network scale and complexity, monitoring the security of a single node or host is no longer sufficient to meet the security needs of the entire network. Therefore, the network security situational awareness system emerged, which can monitor and analyze the entire network in real-time and comprehensively, and analyze and predict the security situation of the network from a global perspective, and has gradually developed into a comprehensive security system that integrates multiple security technologies and means.

The theory of situational awareness was first proposed by the Air Force in the early 1980s. It mainly includes three stages: perception, comprehension, and prediction. Its aim is to better understand the changes in the current combat status of the Air Force, so as to discover, in a timely manner, future situations and make correct responses to ensure the safety of the Air Force. Nowadays, situational awareness technology has been extended to many fields in military operations [4], such as emergency dispatch of air traffic [5], emergency dispatch of medical care [6], and so on.

In 1988, foreign scholar Endsley first proposed the new concept of situational awareness [7], which means that, in a specific time and space domain, by extracting, analyzing, and predicting external environmental factors, one can gain insight into future development trends.

A new concept of group situational awareness [8] was proposed by Wellens in 1993, and it was defined as the consistent view of members of a group on current environmental events. In 1999, Tim Bass first brought the definition of group situational awareness into the field of network security applications [9], and believed that multi-sensor data fusion technology created a critical architecture to enhance the ability of the next-generation intrusion detection system and network security situational awareness system, which can fuse various pieces of data analysis information from multiple heterogeneous IDSs together to accurately determine the identity and danger level of intruders. At present, the academic community still cannot define network security situational awareness with a unified concept, and many theories only further explain the theory concept of situational awareness proposed by Endsley.

Chinese scholars Gong Jian [10] and others re-explained the definition of network security situational awareness and made further clarifications on its research object, proposing that network security situational awareness is a new way of perceiving security situations. It is not simply organizing and stacking security factors on the network, but finding the inherent connections between these security factors and using models supported by various technical conditions, researching the security status of the network according to various user requirements. It aims to obtain comprehensive and integrated security factors in the network environment, incorporate them into data, and have a macroscopic understanding [11]. It is able to make accurate predictions about the network's security situation, which is the best way to ensure that the network remains secure.

As can be seen from the above, network security situational awareness refers to the comprehensive analysis of network activities by collecting and analyzing network data, monitoring environmental changes and network content in different network systems platforms, and thereby obtaining the current security situation of the network, as illustrated in Figure 2. This process can help network security professionals to detect network threats in a timely manner, improve network security prevention and response capabilities, and ensure the stable and secure operation of network systems.

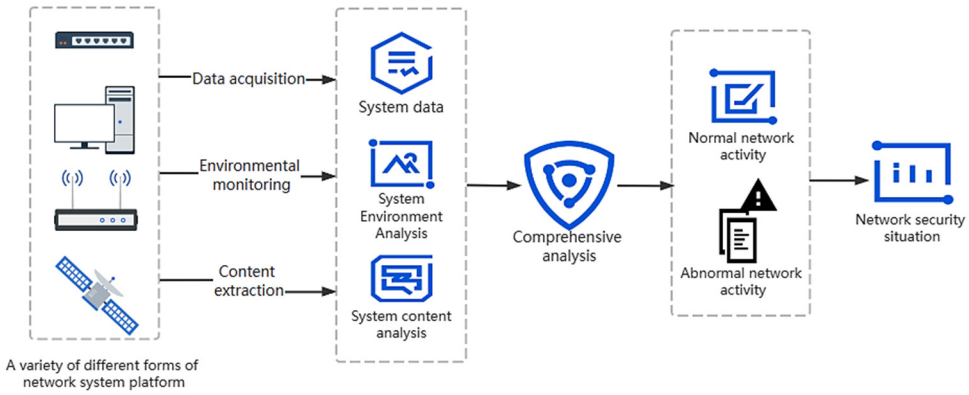

Figure 2. Definition figure of network security situational awareness.

3. The Classic Models of Network Security Situational Awareness

As one of the main research focuses of network security situational awareness, network security situational awareness models can establish a complete situational awareness system, which helps researchers effectively achieve tasks such as situational acquisition, understanding, and prediction. Therefore, researchers have proposed different situational awareness models to cope with different network situations. The following summarizes and categorizes several commonly used classic situational awareness models, including Endsley's three-layer model, the Tim Bass model, JDL model, and OODA control and loop model.

3.1. Endsley's Three-Level Model

The Endsley model [12] was originally applied in the aviation field. As shown in Figure 3, the system first provides corresponding information feedback based on the characteristics of the task, and then performs situational awareness after obtaining feedback information in the decision system. The situational awareness model consists of three layers. The first layer is the acquisition of situation elements, which requires the system to obtain all elements related to network security in the information and preprocess them. The extraction of situation elements provides sufficient and accurate information preparation for the last two layers and is a key factor that affects the processing results of the last two layers. The second layer is situation comprehension. After the acquisition of situation elements in the first layer, this layer continues to sort and analyze the situation elements to obtain the real situation of the current network situation. The third layer is situation prediction, which integrates the results of the first two layers to predict the future network security situation, so as to help network administrators make correct judgments and decisions.

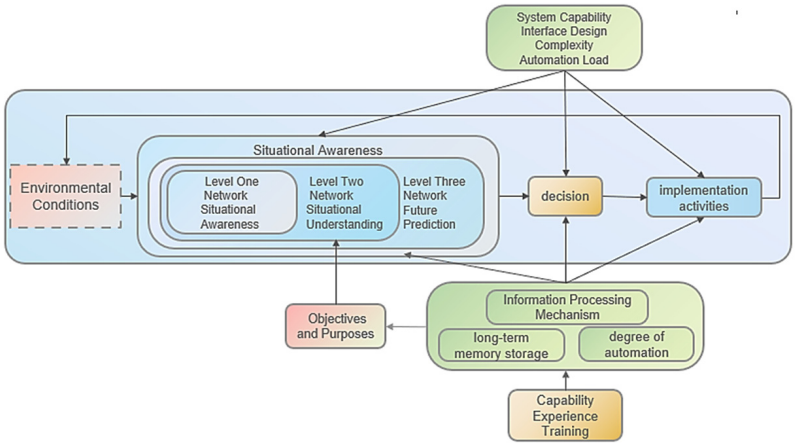

Figure 3. Endsley model.

3.2. JDL Model

Data fusion refers to the process of collecting data from multiple information sources, connecting and cross-combining them to improve the efficiency and accuracy of data analysis. The Joint Directors of Laboratories (JDL) model [13] was proposed by the United States military organization, as shown in Figure 4. The JDL model consists of data sources, data processing, database management systems, and human–computer interfaces, among which data processing is the most important part, divided into five levels to provide a unified framework for data processing in different fields and clearly define the process and function of data processing.

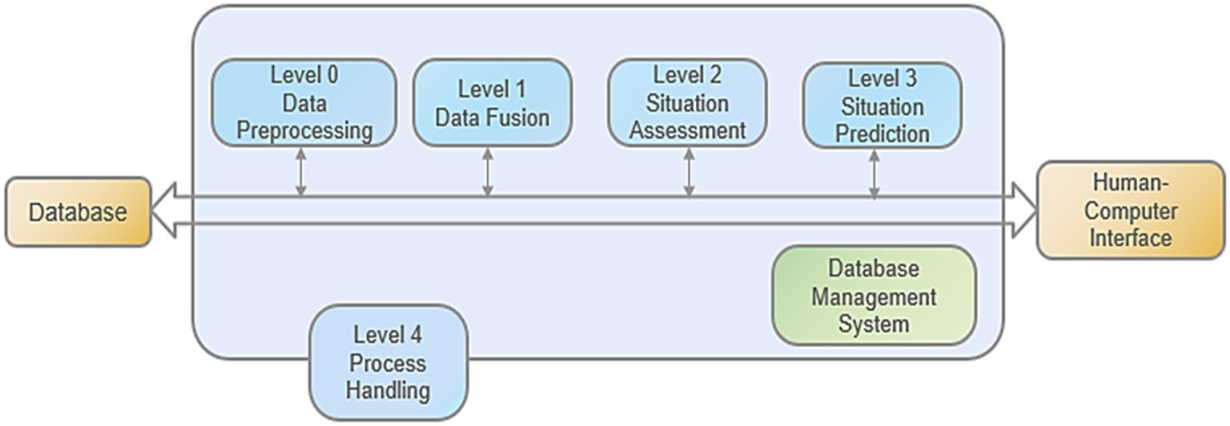

Figure 4. JDL model.

The first layer is data preprocessing. By preprocessing the obtained information, bias can be corrected, and spatial and temporal alignment can be made clearer and more convenient, thus improving the efficiency and accuracy of subsequent operations.

The second layer is data fusion. This layer performs correlation analysis on the data to obtain more accurate target information, so as to make the situation assessment results of the next layer more accurate and reliable.

The third layer is situation assessment. This layer analyzes and understands the data processed by the first two layers as a whole, and then evaluates the current network security situation, providing a reasonable and accurate decision-making basis for network researchers.

The fourth layer is situation prediction. By evaluating the evaluation results obtained from the previous layers, network researchers can predict the future network security situation to better handle security threats.

In the fifth layer, process control is used to control the ongoing data fusion operation. In this way, the entire process of network security situational awareness can be better predicted.

3.3. Tim Bass Model

In 1999, Tim Bass introduced the concept of situational awareness technology into the field of network security. He believed that, to achieve the breakthrough point of the next-generation intrusion detection system, it was necessary to use the information fusion of multi-sensor data to achieve the real-time monitoring and early warning of network situations.

The Tim Bass model [14] was the first to build a network situational awareness framework based on multi-sensor data. It fused data from multiple network security sensors and intrusion detection devices to achieve real-time monitoring of network security, as shown in Figure 5.

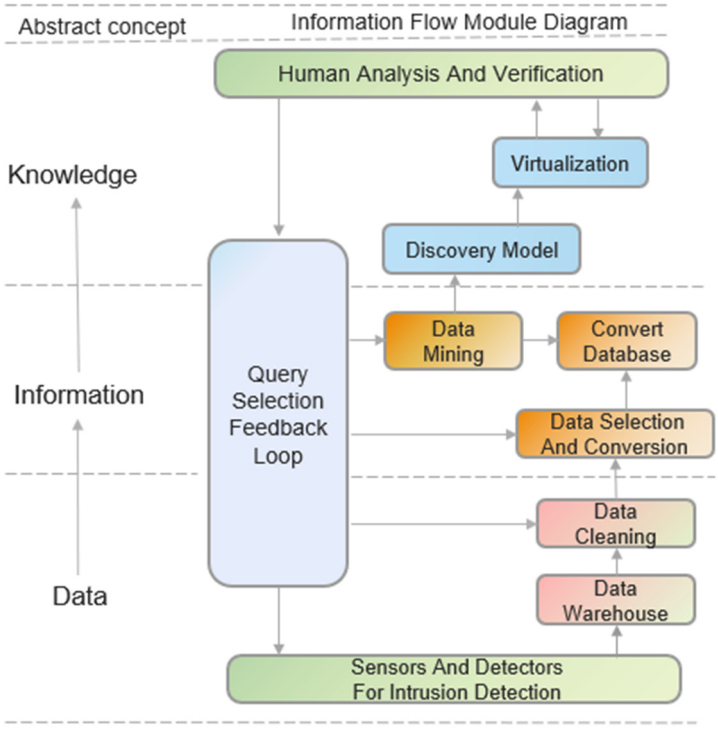

Figure 5. Tim Bass model.

The Data Perception Layer, as the bottom layer of the Tim Bass model, consists of two parts: data collection and preprocessing. These parts are mainly responsible for cleaning and calibrating data, formatting multiple data formats, and studying their correlations. The middle layer organizes and analyzes the data collected from the upper layer to evaluate the network status. The upper layer is responsible for knowledge transformation, predicting major security events that may occur in the current network system, and assessing the current network threat level. The Query Selection and Feedback Loop Unit monitors and evaluates the operation of the entire network system, and co-ordinates the relationships between each layer to ensure the system can operate smoothly, achieve the conversion from data to information to knowledge, and thereby improve the efficiency and reliability of the network.

3.4. OODA Model

The Observe–Orient–Decision–Act (OODA) loop model [15] was proposed by John Boyd, a U.S. Air Force Colonel, in the 1970s based on his experience as a fighter pilot and his research on energy maneuverability. It has been widely applied from its original theoretical foundation on air force strategy to a general strategic approach and to the field of military theory. The OODA loop model describes the process of perceiving purpose and activity, and divides the cycle of situational awareness into four stages—observe, orient, decide, and act—as shown in Figure 6.

The first step is Observation, which mainly uses various sensors to collect data, completing the transition from the physical domain to the information domain. The second stage is Orientation, which studies the data obtained in the first step and summarizes useful key data, thus assisting researchers in making accurate assessments of the corresponding data quickly. The third stage is Decision, in which researchers formulate plans and make decisions based on the judgments made in the second stage. Both judgments and decisions belong to the cognitive domain. The fourth stage is Action, which refers to researchers taking action in the corresponding direction of the decision made in the previous stage, completing the cycle by transitioning from the knowledge domain to the physical domain through action.

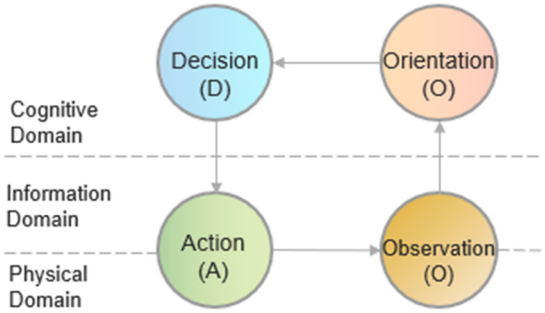

Figure 6. OODA model.

The OODA loop model describes the dynamic execution process of situational awareness. Although it is slightly inferior to the Endsley three-layer model in terms of hierarchy and division of labor, the looping mechanism and dynamic co-ordination of this model can still adapt well to situational awareness in the complex cyberspace.

The above models are all typical situational awareness models. In addition, experts have also provided different situational awareness models to meet the requirements of different application environments and scenarios.

Shen et al. [16] used the Markov game theory to construct a security situational awareness and risk assessment model that integrates intrusion information systems and intrusion defense systems. This model can effectively collect and integrate warning information from both systems. Jia et al. [17] constructed a network security situational awareness model from three aspects, attack, defense, and network security environment, to enhance the effectiveness of network security.

To enhance network security and reduce human intervention, a framework based on the concept of situational awareness is proposed [18], which can provide automation in several steps of the cybersecurity lifecycle and reduce human interaction. The framework includes multiple automated steps that utilize SDN technology to discover entities in the network in real time and assess their vulnerabilities using a Vulnerability Assessment as a Service component. Then, based on the risk level of the entities, they are assigned to appropriate network slices and classified more finely using a machine-learning-based intrusion detection system (IDS) for stronger training results. Finally, real-time data is used for intrusion detection prediction to improve network security and protection efficiency.

4. The Current Research Status of AI-Based Network Security Situational Awareness

4.1. Overview of Artificial Intelligence

Artificial intelligence (AI) is a rapidly growing field of study that focuses on developing theories, methods, technologies, and application systems to simulate, extend, and expand human intelligence. It involves the use of algorithms and computer programs to analyze data, recognize patterns, and make decisions or predictions based on that data. AI has the potential to transform many aspects of modern society, from healthcare and finance to transportation and entertainment. It aims to develop machines that can react quickly in the same way as human intelligence. The research achievements in this field [19–25] involve language and image recognition, medical detection, natural language processing, etc. Not only can AI help us better understand human intelligence, but it can also improve work efficiency and thus enhance our quality of life.

In 1956, the concept of a new generation of artificial intelligence was first proposed at the Dartmouth Conference [26]. Over the next decade, the field made significant progress, achieving noteworthy results in many areas, as shown in Figure 7. However, in the 1970s, despite deep research into the field by many developed countries, the technical challenges faced by artificial intelligence proved difficult to overcome, resulting in slow progress. In the 1990s, with the development of technology, artificial intelligence once again became a hot topic. The emergence of machine learning and algorithms also helped to drive the

development of artificial intelligence. Technology giants joined forces to conduct research and development, making artificial intelligence a focus of widespread attention once again.

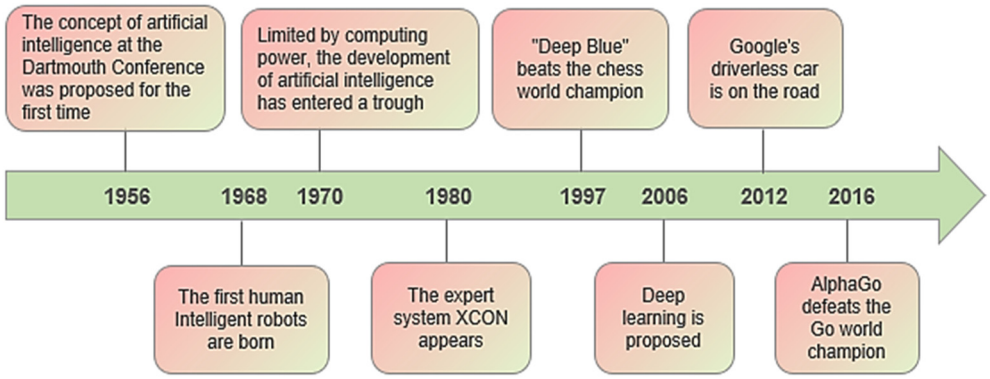

Figure 7. History of artificial intelligence.

There are two different ways in which artificial intelligence can be achieved. One is based on traditional programming techniques, which uses facts and rules to automatically analyze the logical relationships and draw conclusions, such as text recognition and computer chess. The other method involves analyzing data using algorithms and learning from it to make intelligent decisions and predictions, as shown in Figure 8. Unlike traditional coding methods, "training" utilizes massive amounts of data and multiple algorithms to extract effective solutions to complete tasks.

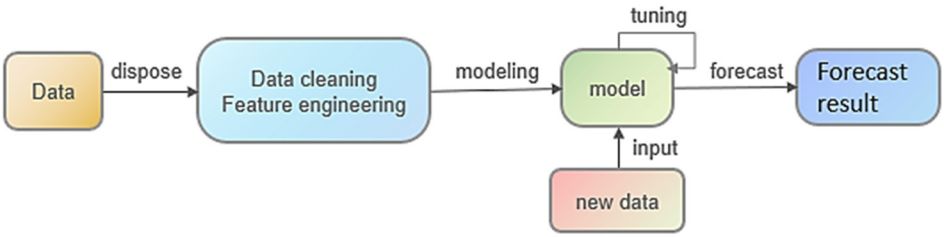

Figure 8. Machine-learning process.

As an important research method in the field of artificial intelligence, machine learning aims to improve the performance of algorithms through empirical learning by running relevant algorithms on a training data set [27,28]. When describing complex and changing security situations, machine-learning algorithms have outstanding adaptability, self-organization, and infinite approximation, which can effectively improve the accuracy of situational assessment and prediction, in order to better cope with complex and changing systems that are variable and nonlinear.

Among them, neural networks are an important research branch in machine learning and can efficiently handle various nonlinear and complex problems [29]. The application of neural network technology in the field of network security has become a hot topic in academia and will be a key direction for future research. This field has important research significance [30,31]. This article mainly introduces several methods of neural networks in situational awareness research, including BP neural networks, wavelet neural networks, RBF neural networks, and LSTM neural networks.

4.2. Current State of Research on Neural-Network-Based Network Security Situational Awareness

4.2.1. BP Neural Network

The backpropagation (BP) neural network is a theoretical model proposed by research scholars, led by Rumelhart and McClelland, in 1986. It uses the method of error backpropagation and trains with a multi-layer feedforward neural network [32]. The forward propagation of signals and the backward propagation of mistakes make up its primary

methodology. That is, when calculating the output error, it follows the direction from input to output; while adjusting the weights and thresholds follows the direction from output to input. Its structure is shown in Figure 9. This structure has an excellent nonlinear mapping ability and a flexible network structure. Depending on the specific situation, the number of intermediate layers and neurons in the network can be flexibly adjusted, and different structural designs can also affect the network's performance.

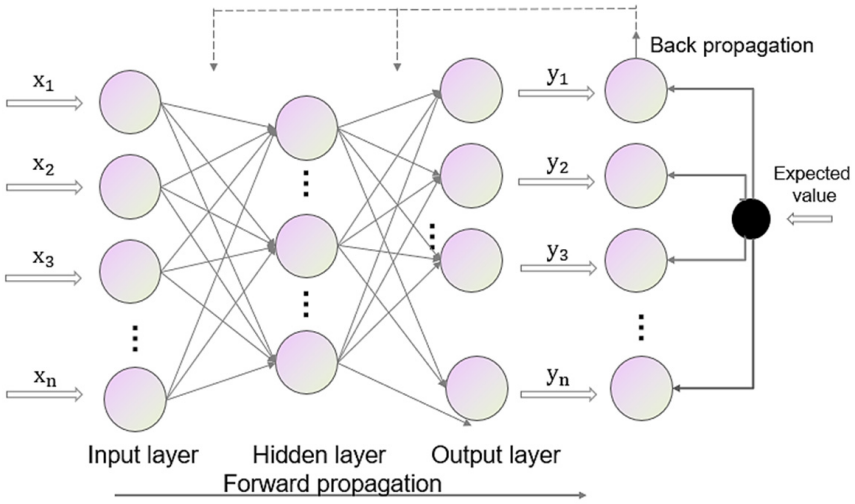

Figure 9. BP neural network structure diagram.

A network security situational assessment algorithm based on the sparrow-search-algorithm-optimized BP neural network is suggested to address the difficulties of low efficiency and poor convergence of standard situational assessment algorithms [33]. The optimal weights and thresholds are determined by this algorithm using the sparrow search algorithm, which are then allocated to the BP neural network to maximize performance. The situational data is then fed into the training algorithm to produce the situational assessment value, and the established network security situational indicator system is used to analyze the dangers to the network system.

Kou G et al. proposed a network security situational element recognition method combining a deep-stacked encoder with the BP algorithm [34]. This method uses unsupervised learning algorithms to train the network layer by layer and obtains a deep-stacked encoder by stacking. The network achieves unsupervised training by employing the encoder to extract the features from the data collection. Simulation studies demonstrate that this approach can successfully enhance the effectiveness and precision of situational awareness.

In addition, Tian Fu et al. [35] proposed to use an adaptive genetic algorithm to effectively optimize the traditional APT attack prediction model, thereby improving prediction accuracy. This model's ability to accurately predict risk nodes that may be present in the network system as well as to track the progress of APT attacks in real time and determine the attack path through sequence attacks greatly enhances the network system's security.

Figure 10 illustrates the CS–BP neural network model that Yin Kun et al. [36] presented for assessing network situational awareness. This model was optimized by the D–S evidence theory. They adapted the conjugate gradient method to the cuckoo search algorithm to speed up training convergence and successfully address the issue of the local minimum in order to enhance the model's local search capability.

A situational assessment model based on SDN networks was proposed by Zhiqiang Du et al. [37]. This model uses an improved algorithm to modify the weights and thresholds of the BP neural network in order to achieve the globally optimal solution and fulfill the objectives of situational assessment and a thorough evaluation of SDN networks.

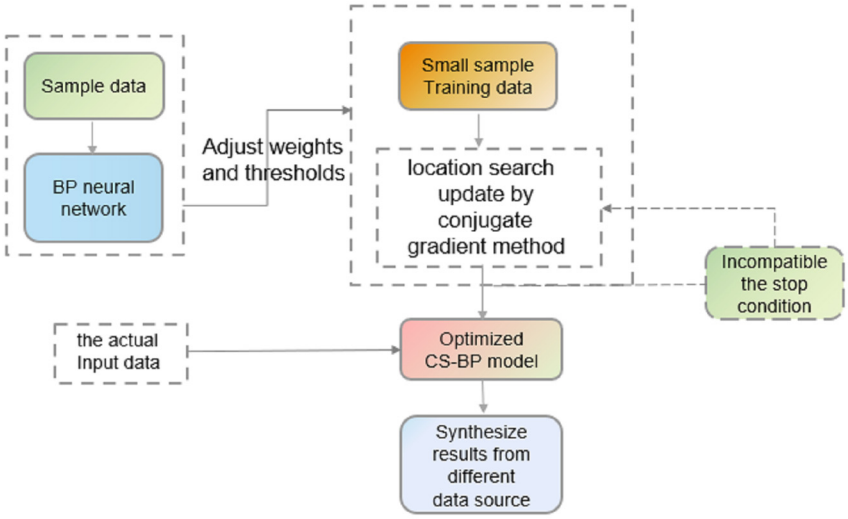

Figure 10. CS–BP neural network flowchart.

4.2.2. Wavelet Neural Network

The wavelet neural network (WNN) has the advantages of a simple structure [38], fast convergence rate, strong learning ability, and high accuracy when processing the same learning tasks, as shown in Figure 11. It can not only guarantee the optimal solution of local details but also achieve the global optimal solution, thus improving the learning efficiency. Based on these advantages of the WNN, people have begun to apply it to the field of network situational awareness, constantly improving and optimizing it, and combining it with genetic algorithms, population optimization algorithms, and other technologies to improve the accuracy and reliability of the model.

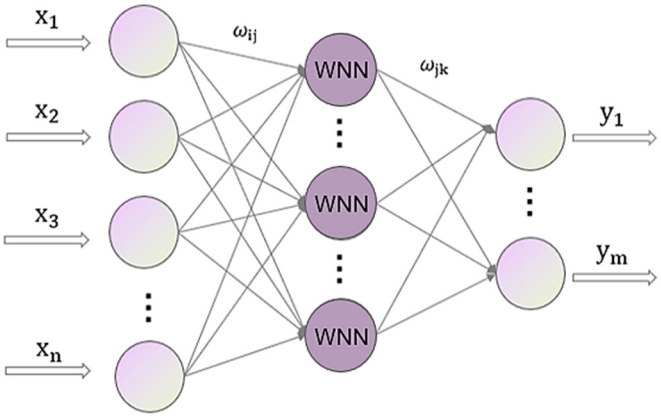

Figure 11. WNN structure diagram.

Using the modified cuckoo search algorithm (MCSA), Ong and colleagues suggested an enhanced initialization method for conventional wavelet neural networks (WNN) [39]. The wavelet hidden nodes' translation vectors are represented by a population of cuckoo eggs in the MCSA algorithm. The cuckoo mimics its own breeding process to improve its positions as it reproduces. The WNN produces its initial transformation vectors using the MCSA solutions. By forecasting the benchmark chaotic time series, this method's viability was assessed, and it outperformed conventional WNN in terms of prediction accuracy.

Huang Cong et al. [40] proposed a new CPSO–DS dynamic wavelet neural network algorithm that can organically combine security information data in heterogeneous systems with the evolution trend of threats to achieve self-adjustment and control management, thereby improving system security and reliability. While achieving the goal of situational

awareness, it can not only supervise and manage the network more effectively, but also provide new effective methods.

For network security situational awareness in power control systems, applying artificial intelligence algorithms based on wavelet neural networks was made [41]. By fusing operational data collecting and integrated processing with scenario index screening and extraction, the sample data set is trained using a wavelet neural network analysis approach. Future state values are anticipated to assist network security employees in making evaluations and judgments by using deep intelligent learning to evaluate the true worth of the network security status.

4.2.3. RBF Neural Network

The radial basis function neural network (RBF neural network) is a type of commonly used three-layer feedforward neural network, as shown in Figure 12. It is a model proposed by Broomhead, Lowe, Moody, and Darken in 1988, which uses radial basis functions in neural networks. The RBF network system [42,43] has the advantages of a simple construction, fast learning rate, excellent approximation performance, and strong generalization ability, making it an ideal choice for complex nonlinear systems, especially for network security situation prediction. By combining the RBF neural network with time series prediction techniques, network security conditions can be effectively predicted, thereby improving network security performance.

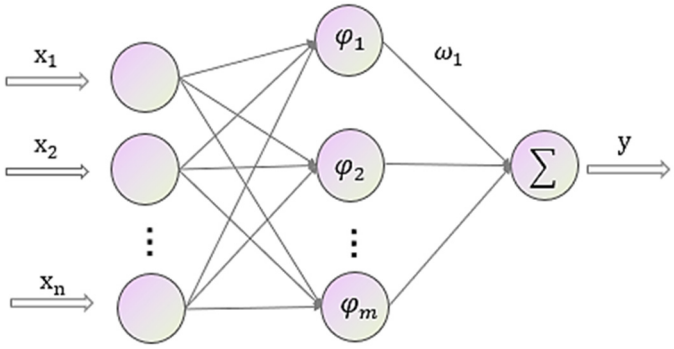

Figure 12. RBF structure diagram.

However, in practical use, neural networks are prone to slow convergence rates, complex network hierarchy designs, and local optimal solution problems. Therefore, many researchers have combined the model structure of RBF neural networks with other technical methods and improved and optimized them.

With the aid of the particle swarm optimization algorithm, Li Yuan et al. [44] enhanced the RBF function neural network and suggested an improved particle swarm optimization–radial basis function algorithm as the prediction model. The findings demonstrated that the enhanced method had a quick convergence rate, high computational efficiency, quick operation time, small error values, and good prediction performance, which are advantageous for advancing network security. By combining the simulated annealing (SA) algorithm with the hybrid hierarchical genetic algorithm (HHGA), Zhihua Chen et al. [45] presented an RBF neural network prediction model based on SA–HHGA optimization. The improved RBF neural network can better maintain network security and has a strong prediction performance.

Then, we put out a fresh methodology for predicting network security conditions that can effectively assess the network security state of small- and medium-sized businesses. The proposed model successfully overcomes the drawback of the RBF gradient descent method easily falling into a local extremum by combining the K-means clustering algorithm and RBF neural network, and using the PSO algorithm to optimize learning parameters such as base width and weight vector. This increases the prediction accuracy of network security situations for enterprises.

4.2.4. Long Short-Term Memory Network

Due to the problem of long-term dependencies in recurrent neural network (RNN) models, they cannot effectively learn features in longer time series. Therefore, to solve this problem, foreign scholars Sepp Hochreiter and Jurgen Schmidhuber designed long short-term memory networks (LSTM) as an improvement solution [46], with the expectation of effectively alleviating this problem.

The recurrent neural network (RNN) is composed of repeating neural network modules, each module containing only one tanh layer. It calculates the current output based on the current input and the previous output from the last time step, as shown in Figure 13. The long short-term memory network (LSTM) is a special type of RNN that effectively solves the problem of long-term dependencies [47]. After improvement, the structure of the LSTM is more flexible and efficient, as shown in Figure 14. The structure of the LSTM is similar to RNN, but the repeating modules are more complex.

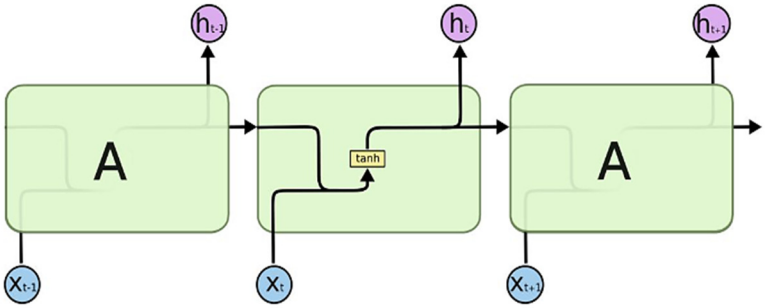

Figure 13. RNN structure diagram.

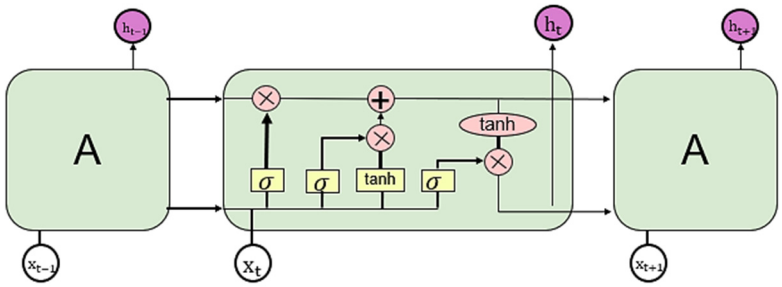

Figure 14. LSTM structure diagram.

Haofang Zhang et al. [48] combined the decision tree algorithm (DT) with long short-term memory (LSTM) networks to construct an LSTM–DT model. The model predicts attack probability using the LSTM network on processed data sets while using the DT algorithm to identify attack types. This model provides better risk assessment indicators and quantification methods for describing complex network environment problems.

By combining fractal theory with evolutionary algorithm optimization, we created a fractal neural network (FNN) to address gradient explosion or disappearance concerns [49]. Their situational awareness and prediction model for network security used LSTM networks as its main structural component. The viability and effectiveness of neural network structures for situational awareness and prediction in network security are improved by employing the fractal differential function as the activation function, according to experimental results.

Qi Wang et al. [50] proposed a novel situational awareness (SA) model by aggregating convolutional neural networks (CNN) and long short-term memory (LSTM) recurrent neural networks, which has some advantages in the co-data mining of spatiotemporal measurement data. The CNN–LSTM module provided in the model simultaneously learns spatial and temporal features from the phasor measurement unit data. The SA model is designed with two functional branches, an emergency locator for monitoring the exact

location of current faults, and a stability predictor for predicting the future stable performance of the system. Test results showed the high performance (accuracy) of the model even in situations with low data adequacy. The proposed SA model is expected to promote quick actions by system operators after faults to prevent any unstable operating states in the power system.

5. Implementation and Application

Network security situational awareness is at the core of modern network security defense. This paper will introduce several key aspects of network security situational awareness from the perspective of implementation and application, including vulnerability scanning and management, behavior analysis and anomaly detection, and security incident response and management. These applications and implementation methods can help enterprises and organizations protect their network security more comprehensively and effectively, and prevent and respond to various security threats.

5.1. Vulnerability Scanning and Management

In today's internet environment, network attacks and security vulnerabilities have become increasingly important concerns for enterprises and organizations. As network attacks become more complex and frequent, enterprises and organizations need a comprehensive and efficient method to identify and fix network vulnerabilities in order to ensure the security of their networks. Through vulnerability scanning, network administrators can identify various vulnerabilities that exist in the network, categorize and record them, and then use vulnerability management tools to track and fix these vulnerabilities. The goal of vulnerability scanning and management is to ensure the integrity, availability, and confidentiality of the network, and to help enterprises and organizations avoid data leaks and other security threats [51,52].

Vulnerability control (VULCON) was created and evaluated as a successful vulnerability management technique based on two essential performance indicators: time to vulnerability remediation (TVR) and total vulnerability exposure (TVE) [53]. VULCON incorporates true vulnerability scanning reports, information about found vulnerabilities, asset criticality, and human resource metadata. It then employs a mixed-integer multi-objective optimization method to prioritize patching vulnerabilities in order to optimize the aforementioned performance metrics under specified resource restrictions. VULCON provides useful operational assistance for optimizing the vulnerability response process in a network security operations center.

Because software vulnerabilities have always posed a danger to the reliability of public and critical infrastructure, many studies have been dedicated to detecting and mitigating software faults [54], the majority of which use static and dynamic analysis [55,56]. These techniques do have certain disadvantages, though, such as a lot of manual labor and intricacy. A deep-learning-based VulANalyzeR model is proposed for automated binary vulnerability detection, classification of common vulnerability enumeration types, and root cause analysis to improve security, in order to address the issue where current solutions cannot capture the complex relationships between various variables from raw binary code [57]. To simulate programme execution, attention mechanisms are included throughout the model for sequential and topological learning via recurrent units and graph convolution. It also uses multitask learning to classify certain vulnerability categories, which not only provides further explanations but also allows zero-day vulnerabilities to be corrected more quickly.

Because patching all susceptible machines in an enterprise or organization at once is unrealistic, patch priorities can be established first. By ranking vulnerabilities in the planning graph, Olswang et al. proposed using network topology vulnerability scoring (NTVS) to provide more desirable outcomes [58]. When analyzing logical attack graphs, planners employ the planning graph as a temporary data structure. The key findings from two real-world networks show that patching vulnerabilities with a higher NTVS priority

reduces the number of possible attack pathways against critical assets faster. As a result, the proposed visualization can assist specialists in determining the priority of vulnerability patches and explaining their conclusions to upper management and operations teams.

5.2. Behavioral Analysis and Anomaly Detection

Behavioral analysis and anomaly detection can improve network security effectiveness and accuracy by analyzing and monitoring the behavior patterns of users and devices in the network, and identifying potential security threats and abnormal behavior [59,60]. This method is widely used in fields such as intrusion detection and malware detection.

In the network, encrypted traffic is mainly identified for subsequent intrusion detection and malware detection. Because many network attackers use encryption to conceal their attacks, identifying encrypted traffic is crucial for effective intrusion detection and malware detection. Once encrypted traffic is identified, intrusion detection systems can use intrusion detection rules to detect attack behavior and take corresponding measures upon discovering attacks. Malware detection systems can detect malware by examining malicious software indicators in encrypted traffic.

In today's complex network environment, traditional methods of capturing patterns and keywords from payloads in data packets are no longer applicable [61,62]. More and more research is using machine-learning and deep-learning technologies for encrypted traffic classification [63–68]. The advantage of deep learning over traditional machine learning is its ability to handle more complex tasks and data with higher accuracy and adaptability. Deep learning uses neural network models to automatically extract features and perform classification, avoiding the laborious and inaccurate manual feature extraction. In addition, deep learning can handle large amounts of data, learn statistical regularities in the data more effectively, and improve the generalization ability of the model. The flowchart of deep learning is shown in the Figure 15.

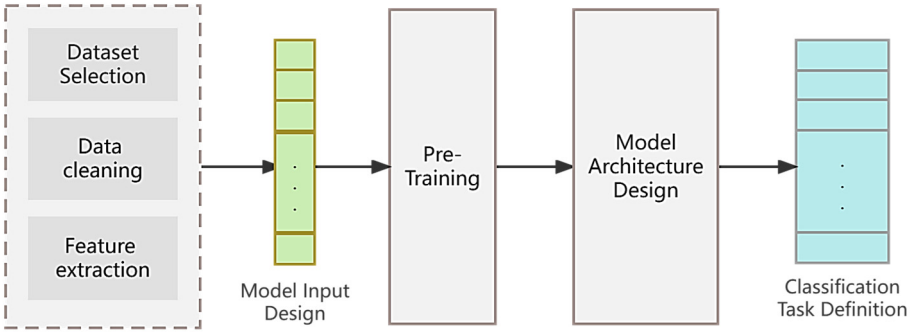

Figure 15. The flowchart of deep learning.

The emergence of pretrained models has brought better performance to the task of encrypted traffic classification. The transformer, a neural network model based on attention mechanisms, as shown in Figure 16, was initially applied in the field of natural language processing [69], but has been successfully applied in computer networks in recent years. Compared with traditional convolutional neural networks and recurrent neural networks, the transformer model can use a large amount of unlabeled data to improve classification accuracy and generalization capability, and has a better parallel computing performance and stronger modeling ability [70,71], which can better capture the temporal relationships and long-distance dependencies in traffic, and thus performs well in traffic classification tasks [72–74].

Based on the pretrained transformer model, a method for encrypted traffic classification called ET–BERT was proposed [75]. This method represents packets in vector form and then uses the pretrained BERT model to process these vectors and extract meaningful features; the BERT model is shown in Figure 17. Finally, these features are input into a classifier for classification. Peng Lin et al. designed a novel multimodal deep learning

framework called PEAN [65], which uses raw byte and length sequences as inputs and uses self-attention mechanisms to learn deep relationships between network packets. In addition, unsupervised pretraining is introduced to enhance PEAN's ability to represent network packets, and experiments conducted on a large-scale data set of real traces captured in data centers have demonstrated the effectiveness of PEAN.

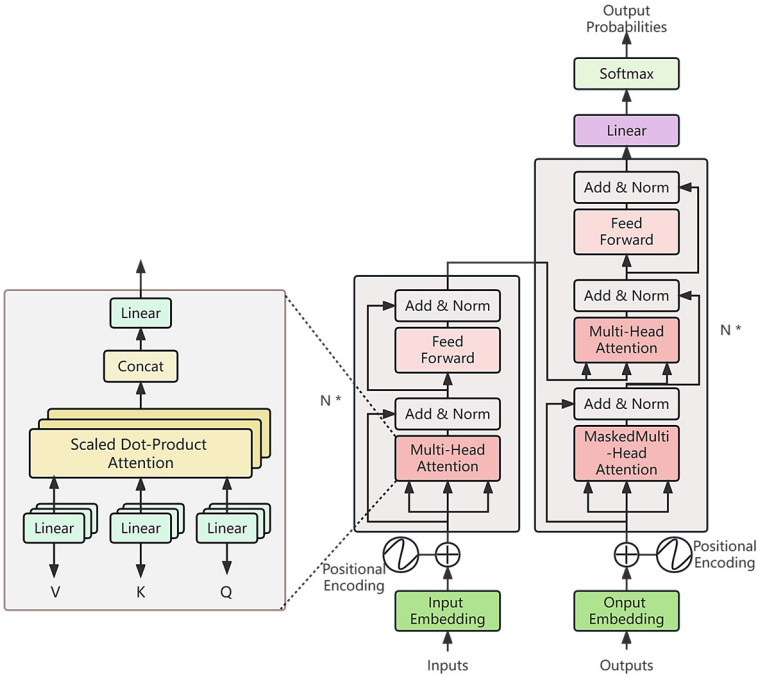

Figure 16. Transformer architecture diagram.

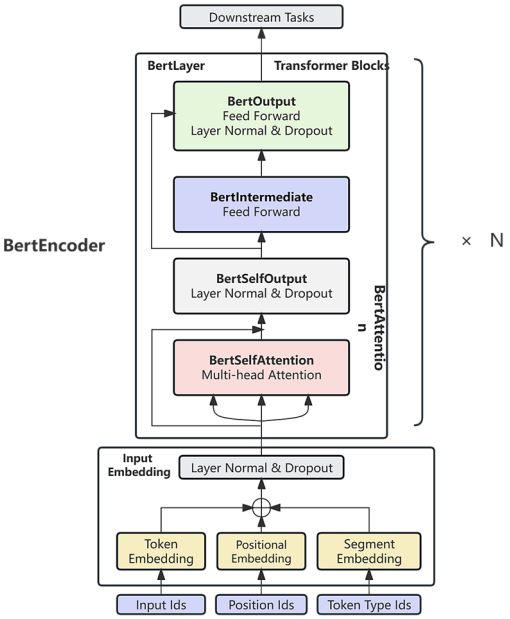

Figure 17. Bert architecture diagram.

5.3. Security Incident Response and Management

Security incident response and management is a crucial part of network security situational awareness. It refers to the quick, accurate, and effective response and management of security incidents such as malicious attacks, exploitation of vulnerabilities, and data leaks, once they are detected. Security incident response and management is an active

defense method, whose purpose is to detect and respond to security incidents as quickly as possible, in order to minimize the losses caused by security incidents and protect the security of information systems and users [76–78].

Security incident response and management mainly consists of the following steps [79]: The first is event monitoring and identification, which is a critical step in identifying potential security incidents. Next is event analysis and classification, which involves the further analysis of events to determine their sources, types, and levels of harm. Then, there is event response and disposal, which involves taking the appropriate response and disposal measures based on the urgency and level of harm of the event. Finally, there is event evaluation and summary, which involves evaluating and summarizing the results of event handling, in order to improve security incident response and management strategies.

In network security situational awareness, security incident response and management need to work in co-ordination with other modules, such as threat intelligence collection and analysis, vulnerability management, and anomaly detection. Only by working in co-ordination with these modules can network security be better protected.

6. Summary and Future Directions

This article summarizes the relevant work on network security situational awareness, with a focus on artificial intelligence. The concept and classical models of network security situational awareness are specifically elaborated, and artificial intelligence is introduced accordingly. Starting from machine-learning-based methods, the current research status of neural-network-based network security situational awareness is discussed, and recent research work is summarized.

As information technology matures, the number and complexity of network security risks faced by networks are increasing, and the attack methods are becoming more diversified. Consequently, it is becoming increasingly difficult to deal with various risk events on the Internet. The following analysis and outlook will be made on the development trend of current network security situational awareness:

(1) Integration with new research fields

Traditional network situational awareness is usually designed to address relatively traditional network threats such as network viruses, malware, and encrypted traffic. However, with the development of emerging fields, network security situational awareness will not be limited to traditional network threats, but will be expanded to new areas such as cloud computing and edge computing.

(2) Integration with new technological developments

When it comes to the future development of network security situational awareness, the integration with new technologies is a promising direction to explore. For instance, the development of artificial intelligence, big data, and blockchain technologies have brought new solutions and ideas to network security. By integrating these technologies with network security situational awareness, it is possible to further enhance the accuracy, real-time nature, and intelligence level of network security, thus better protecting network security.

(3) Integration with visualization display

Visualization display is the intuitive display of the important information and analysis results hidden in the massive data of network security situational awareness, which helps decision makers to understand and analyze data more clearly and effectively and make corresponding decisions. Nowadays, we have entered the era of big data, and the original methods cannot meet the needs of information communication in large data sets. A large amount of dynamic information can only be conveyed through more efficient processing and expression forms. Therefore, how to construct an efficient and interactive big data analysis and visualization method to convey large-scale real-time information data has become a key exploration in data analysis and visualization.

Overall, the research work of situational awareness is still in its infancy, and there are still many aspects that need to be improved and developed. However, with the continuous

improvement of related technologies and research, more perfect mathematical models will be constructed, more scientific evaluation methods will be adopted, and the advantages and characteristics of situational awareness will be fully utilized to achieve more effective protection of network security.

Author Contributions: Conceptualization, M.W. and G.S.; methodology, Y.Y. and B.Z.; formal analysis, M.W.; investigation, G.S.; writing, original draft preparation, M.W. and G.S.; supervision, M.W.; project administration, M.W.; visualization, G.S. and Y.Y.; writing—review and editing, G.S., Y.Y. and B.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: This review has no information related to it.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AI	Artificial Intelligence
CNNIC	China Internet Network Information Center
IDS	Intrusion Detection Systems
JDL	Joint Directors of Laboratories
OODA	Observe–Orient–Decision–Act
BP	Backpropagation
SDN	Software-Defined Network
WNN	Wavelet Neural Network
MCSA	Modified Cuckoo Search Algorithm
RBF	Radial Basis Function
HHGA	Hybrid Hierarchical Genetic Algorithm
PSO	Particle Swarm Optimization
CNN	Convolutional Neural Networks
RNN	Recurrent Neural Network
LSTM	Long Short-Term Memory
SA	Situational Awareness
IDS	Intrusion Detection Systems
VULCON	Vulnerability Control
TVR	Time to Vulnerability Remediation
TVE	Total Vulnerability Exposure
NTVS	Network Topology Vulnerability Scoring
BERT	Bidirectional Encoder Representations from Transformers

References

1. Denning, D.E. An Intrusion-Detection Model. *IEEE Trans. Softw. Eng.* **1987**, *SE-13*, 222–232. [CrossRef]
2. Vigna, G.; Kemmerer, R.A. NetSTAT: A network-based intrusion detection system. *J. Comput. Secur.* **1999**, *7*, 37–71. [CrossRef]
3. Mukherjee, B.; Heberlein, L.T.; Levitt, K.N. Network intrusion detection. *IEEE Netw.* **1994**, *8*, 26–41. [CrossRef]
4. Lenders, V.; Tanner, A.; Blarer, A. Gaining an edge in cyber space with advanced situational awareness. *IEEE Secur. Priv.* **2015**, *13*, 65–74. [CrossRef]
5. Friedrich, M.; Biermann, M.; Gontar, P.; Biella, M.; Bengler, K. The influence of task load on situation awareness and control strategy in the ATC tower environment. *Cogn. Technol. Work.* **2018**, *20*, 205–217. [CrossRef]
6. Green, B.; Parry, D.; Oeppen, R.S.; Plint, S.; Dale, T.; Brennan, P.A. Situational awareness—What it means for clinicians, its recognition and importance in patient safety. *Oral Dis.* **2017**, *23*, 721–725. [CrossRef]
7. Eggemeier, F.T.; Crabtree, M.S.; LaPointe, P.A. The effect of delayed report on subjective ratings of mental workload. In Proceedings of the Human Factors Society Annual Meeting (27th) on the Effect of Delayed Report on Subjective Ratings of Mental Workloads, Norkfolk, VA, USA, 10–14 October 1983.
8. Wellens, A.R. Group Situation Awareness and Distributed Decision Making: From Military to Civilian Applications. In *Individual and Group Decision Making: Current Issues*; Lawrence Erlbaum Associates, Inc.: Hillsdale, NJ, USA, 1993; pp. 267–291.
9. Bass, T.; Gruber, D. A glimpse into the future of ID. *Mag. USENIX SAGE* **1999**, *24*, 40–49.
10. Gong, J.; Zang, X.-D.; Su, Q.; Hu, X.-Y.; Xu, J. Survey of network security situation awareness. *J. Softw.* **2016**, *28*, 1010–1026.
11. Shi, L.; Liu, J.; Liu, Y.; Zhu, H.; Duan, P. Review of network security situational awareness. *Comput. Eng. Appl.* **2019**, *55*, 1–9.

12. Endsley, M.R. Situation awareness global assessment technique (SAGAT). In Proceedings of the IEEE 1988 National Aerospace and Electronics Conference, Dayton, OH, USA, 23–27 May 1988; pp. 789–795.
13. Hall, D.L.; Llinas, J. An introduction to multisensor data fusion. *Proc. IEEE* **1997**, *85*, 6–23. [CrossRef]
14. Bass, T.; Robichaux, R. Defense-in-depth revisited: Qualitative risk analysis methodology for complex network-centric operations. In Proceedings of the MILCOM Proceedings Communications for Network-Centric Operations: Creating the Information Force (Cat. No. 01CH37277), McLean, VA, USA, 28–31 October 2001; Volume 1, pp. 64–70.
15. Boyd, J. *A Discourse on Winning and Losing*; Air University Press: Maxwell Air Force Base, AL, USA, 2018; p. 347.
16. Shen, D.; Chen, G.; Cruz, J.B., Jr.; Haynes, L.; Kruger, M.; Blasch, E. A markov game theoretic data fusion approach for cyber situational awareness. In *Multisensor, Multisource Information Fusion: Architectures, Algorithms, and Applications*; SPIE: Bellingham, WA, USA, 2007; Volume 6571, pp. 143–154.
17. Jia, X.F.; Liu, Y.; Yan, Y.; Wu, D. Network security situational awareness method based on capability-opportunity-intent model. *Appl. Res. Comput.* **2016**, *6*, 1775–1779.
18. Nikoloudakis, Y.; Kefaloukos, I.; Klados, S.; Panagiotakis, S.; Pallis, E.; Skianis, C.; Markakis, E.K. Towards a machine learning based situational awareness framework for cybersecurity: An SDN implementation. *Sensors* **2021**, *21*, 4939. [CrossRef]
19. Aggarwal, K.; Mijwil, M.M.; Al-Mistarehi, A.H.; Alomari, S.; Gök, M.; Alaabdin, A.M.Z.; Abdulrhman, S.H. Has the future started? The current growth of artificial intelligence, machine learning, and deep learning. *Iraqi J. Comput. Sci. Math.* **2022**, *3*, 115–123.
20. Jain, A.; Tiwari, S. Prediction and Visualisation of Viral Genome Antigen Using Deep Learning & Artificial Intelligence. In Proceedings of the 2021 5th International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 8–10 April 2021; pp. 1430–1437.
21. Kothari, D.; Patel, M.; Sharma, A.K. Implementation of Grey Scale Normalization in Machine Learning & Artificial Intelligence for Bioinformatics using Convolutional Neural Networks. In Proceedings of the 2021 6th International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India, 20–22 January 2021; pp. 1071–1074.
22. Visvikis, D.; Cheze Le Rest, C.; Jaouen, V.; Hatt, M. Artificial intelligence, machine (deep) learning and radio (geno) mics: Definitions and nuclear medicine imaging applications. *Eur. J. Nucl. Med. Mol. Imaging* **2019**, *46*, 2630–2637. [CrossRef]
23. Aggour, K.S.; Gupta, V.K.; Ruscitto, D.; Ajdelsztajn, L.; Bian, X.; Brosnan, K.H.; Kumar, N.C.; Dheeradhada, V.; Hanlon, T.; Iyer, N.; et al. Artificial intelligence/machine learning in manufacturing and inspection: A GE perspective. *MRS Bull.* **2019**, *44*, 545–558. [CrossRef]
24. Ali, D.; Frimpong, S. Artificial intelligence, machine learning and process automation: Existing knowledge frontier and way forward for mining sector. *Artif. Intell. Rev.* **2020**, *53*, 6025–6042. [CrossRef]
25. Cioffi, R.; Travaglioni, M.; Piscitelli, G.; Petrillo, A.; De Felice, F. Artificial intelligence and machine learning applications in smart production: Progress, trends, and directions. *Sustainability* **2020**, *12*, 492. [CrossRef]
26. Haenlein, M.; Kaplan, A. A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence. *Calif. Manag. Rev.* **2019**, *61*, 5–14. [CrossRef]
27. Ongsulee, P. Artificial intelligence, machine learning and deep learning. In Proceedings of the 2017 15th International Conference on ICT and Knowledge Engineering (ICT&KE), Bangkok, Thailand, 22–24 November 2017; pp. 1–6.
28. Xin, Y.; Kong, L.; Liu, Z.; Chen, Y.; Li, Y.; Zhu, H.; Gao, M.; Hou, H.; Wang, C. Machine learning and deep learning methods for cybersecurity. *IEEE Access* **2018**, *6*, 35365–35381. [CrossRef]
29. Shinde, P.P.; Shah, S. A review of machine learning and deep learning applications. In Proceedings of the 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), Pune, India, 16–18 August 2018; pp. 1–6.
30. Yang, H.; Zeng, R.; Xu, G.; Zhang, L. A network security situation assessment method based on adversarial deep learning. *Appl. Soft Comput.* **2021**, *102*, 107096. [CrossRef]
31. Geluvaraj, B.; Satwik, P.M.; Ashok Kumar, T.A. The future of cybersecurity: Major role of artificial intelligence, machine learning, and deep learning in cyberspace. In Proceedings of the International Conference on Computer Networks and Communication Technologies: ICCNCT 2018, Bengaluru, India, 10–12 July 2018; Springer: Singapore, 2019; pp. 739–747.
32. Rumelhart, D.E.; Hinton, G.E.; Williams, R.J. Learning representations by back-propagating errors. *Nature* **1986**, *323*, 533–536. [CrossRef]
33. Zhang, R.; Pan, Z.; Yin, Y. Research on assessment algorithm for network security situation based on SSA-BP neural network. In Proceedings of the 2021 7th International Symposium on System and Software Reliability (ISSSR), Chongqing, China, 23–24 September 2021; pp. 140–145.
34. Kou, G.; Wang, S.; Zhang, D. Recognition of network security situation elements based on depth stack encoder and back propagation algorithm. *J. Electron. Inf. Technol.* **2019**, *41*, 2187–2193.
35. Fu, T.; Lu, Y.; Zhen, W. APT attack situation assessment model based on optimized BP neural network. In Proceedings of the 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (IT-NEC), IEEE, Chengdu, China, 15–17 March 2017; pp. 2108–2111.
36. Yin, K.; Yang, Y.; Yang, J.; Yao, C. A network security situation assessment model based on BP neural network optimized by DS evidence theory. *J. Phys. Conf. Ser.* **2022**, *2258*, 012039. [CrossRef]
37. Du, Z.; Yao, H.; Fu, Y.; Cao, Z.; Liang, H.; Ren, J. Network Situation Assessment Method Based on Improved BP Neural Network. *Electronics* **2023**, *12*, 483. [CrossRef]

38. Alexandridis, A.K.; Zapranis, A.D. Wavelet neural networks: A practical guide. *Neural Netw.* **2013**, *42*, 1–27. [CrossRef]
39. Ong, P.; Zainuddin, Z. Optimizing wavelet neural networks using modified cuckoo search for multi-step ahead chaotic time series prediction. *Appl. Soft Comput.* **2019**, *80*, 374–386. [CrossRef]
40. Huang, C.; Wang, C. Network Security Situation Awareness Based on the Optimized Dynamic Wavelet Neural Network. *Int. J. Netw. Secur.* **2018**, *20*, 593–600.
41. Zhao, J.; Li, X.; Cao, Y.; Liu, J.; Yan, J.; Li, C. Analysis and Application of intelligent Power Control System Cyber Security Situation Awareness Based on Wavelet Neural Network. *J. Phys. Conf. Ser.* **2021**, *2078*, 012067. [CrossRef]
42. Hwang, Y.S.; Bang, S.Y. An efficient method to construct a radial basis function neural network classifier. *Neural Netw.* **1997**, *10*, 1495–1503. [CrossRef]
43. Xie, T.; Yu, H.; Wilamowski, B. Comparison between traditional neural networks and radial basis function networks. In Proceedings of the 2011 IEEE International Symposium on Industrial Electronics, Gdansk, Poland, 27–30 June 2011; pp. 1194–1199.
44. Li, Y. Prediction of network security situation awareness based on an improved model combined with neural network. *IEEE Secur. Priv.* **2021**, *4*, e181.
45. Chen, Z. Research on Internet Security Situation Awareness Prediction Technology Based on Improved RBF Neural Network Algorithm. *J. Comput. Cogn. Eng.* **2022**, *1*, 103–108.
46. Hochreiter, S.; Schmidhuber, J. Long Short-Term Memory. *Neural Comput.* **1997**, *9*, 1735–1780. [CrossRef]
47. Van Houdt, G.; Mosquera, C.; Nápoles, G. A review on the long short-term memory model. *Artif. Intell. Rev.* **2020**, *53*, 5929–5955. [CrossRef]
48. Zhang, H.; Kang, C.; Xiao, Y. Research on Network Security Situation Awareness Based on the LSTM-DT Model. *Sensors* **2021**, *21*, 4788. [CrossRef]
49. Ding, C.; Chen, Y.; Algarni, A.M.; Zhang, G.; Peng, H. Application of fractal neural network in network security situation awareness. *World Sci.* **2022**, *2*, 2240090. [CrossRef]
50. Wang, Q.; Bu, S.; He, Z.; Yangdong, Z. Toward the Prediction Level of Situation Awareness for Electric Power Systems Using CNN-LSTM Network. *IEEE Trans. Ind. Inform.* **2021**, *17*, 6951–6961. [CrossRef]
51. Shu, X.; Tian, K.; Ciambrone, A.; Yao, D. Breaking the target: An analysis of target data breach and lessons learned. *arXiv* **2017**, arXiv:1701.04940.
52. Alexopoulos, N.; Habib, S.M.; Schulz, S.; Mühlhäuser, M. The tip of the iceberg: On the merits of finding security bugs. *ACM Trans. Priv. Secur.* **2020**, *24*, 3. [CrossRef]
53. Farris, K.A.; Shah, A.; Cybenko, G.; Ganesan, R.; Jajodia, S. Vulcon: A system for vulnerability prioritization, mitigation, and management. *ACM Trans. Priv. Secur.* **2018**, *21*, 16. [CrossRef]
54. Dissanayake, N.; Jayatilaka, A.; Zahedi, M.; Babar, M.A. Software security patch management—A systematic literature review of challenges, approaches, tools and practices. *Inf. Softw. Technol.* **2022**, *144*, 106771. [CrossRef]
55. Nunes, P.; Medeiros, I.; Fonseca, J.; Neves, N.; Correia, M.; Vieira, M. On combining diverse static analysis tools for web security: An empirical study. In Proceedings of the 2017 13th European Dependable Computing Conference (EDCC), Geneva, Switzerland, 4–8 September 2017; pp. 121–128.
56. Nunes, P.J.C.; Fonseca, J.; Vieira, M. phpSAFE: A security analysis tool for OOP web application plugins. In Proceedings of the 2015 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, Rio de Janeiro, Brazil, 22–25 June 2015; pp. 299–306.
57. Li, L.; Ding, S.H.; Tian, Y.; Fung, B.C.; Charland, P.; Ou, W.; Song, L.; Chen, C. VulANalyzeR: Explainable Binary Vulnerability Detection with Multi-task Learning and Attentional Graph Convolution. *ACM Trans. Priv. Secur.* **2023**, *26*, 3. [CrossRef]
58. Olswang, A.; Gonda, T.; Puzis, R.; Shani, G.; Shapira, B.; Tractinsky, N. Prioritizing vulnerability patches in large networks. *Expert Syst. Appl.* **2022**, *193*, 116467. [CrossRef]
59. Zhang, X.; Wang, T. Elastic and reliable bandwidth reservation based on distributed traffic monitoring and control. *IEEE Trans. Parallel Distrib. Syst.* **2022**, *33*, 4563–4580. [CrossRef]
60. Zhang, X.; Wang, Y.; Yang, M.; Geng, G. Toward concurrent video multicast orchestration for caching-assisted mobile networks. *IEEE Trans. Veh. Technol.* **2021**, *70*, 13205–13220. [CrossRef]
61. Finsterbusch, M.; Richter, C.; Rocha, E.; Muller, J.A.; Hanssgen, K. A survey of payload-based traffic classification approaches. *IEEE Commun. Surv. Tutor.* **2013**, *16*, 1135–1156. [CrossRef]
62. Roughan, M.; Sen, S.; Spatscheck, O.; Duffield, N. Class-of-service mapping for QoS: A statistical signature-based approach to IP traffic classification. In Proceedings of the 4th ACM SIGCOMM Conference on Internet Measurement, Sicily, Italy, 25–27 October 2004; pp. 135–148.
63. Rezaei, S.; Liu, X. Deep learning for encrypted traffic classification: An overview. *IEEE Commun. Mag.* **2019**, *57*, 76–81. [CrossRef]
64. Aceto, G.; Ciuonzo, D.; Montieri, A.; Pescapé, A. DISTILLER: Encrypted traffic classification via multimodal multitask deep learning. *J. Netw. Comput. Appl.* **2021**, *183*, 102985. [CrossRef]
65. Lin, P.; Ye, K.; Hu, Y.; Lin, Y.; Xu, C.Z. A Novel Multimodal Deep Learning Framework for Encrypted Traffic Classification. *IEEE/ACM Trans. Netw.* **2022**. early access. [CrossRef]
66. Pacheco, F.; Exposito, E.; Gineste, M.; Baudoin, C.; Aguilar, J. Towards the deployment of machine learning solutions in network traffic classification: A systematic survey. *IEEE Commun. Surv. Tutor.* **2018**, *21*, 1988–2014. [CrossRef]

67. Montieri, A.; Ciuonzo, D.; Aceto, G.; Pescapé, A. Anonymity services tor, i2p, jondonym: Classifying in the dark (web). *IEEE Trans. Dependable Secur. Comput.* **2018**, *17*, 662–675. [CrossRef]
68. Wang, L.; Mei, H.; Sheng, V.S. Multilevel identification and classification analysis of Tor on mobile and PC platforms. *IEEE Trans. Ind. Inform.* **2020**, *17*, 1079–1088. [CrossRef]
69. Vaswani, A.; Shazeer, N.; Parmar, N.; Uszkoreit, J.; Jones, L.; Gomez, A.N.; Kaiser, Ł.; Polosukhin, I. Attention is all you need. Advances in neural information processing systems. *arXiv* **2017**, arXiv:1706.03762.
70. Devlin, J.; Chang, M.W.; Lee, K.; Toutanova, K. Bert: Pre-training of deep bidirectional transformers for language understanding. *arXiv* **2018**, arXiv:1810.04805.
71. Radford, A.; Narasimhan, K.; Salimans, T.; Sutskever, I. Improving Language Understanding by Generative Pre-Training. 2018. Available online: https://www.cs.ubc.ca/~amuham01/LING530/papers/radford2018improving.pdf (accessed on 7 March 2023).
72. Zhao, R.; Deng, X.; Yan, Z.; Ma, J.; Xue, Z.; Wang, Y. MT-FlowFormer: A Semi-Supervised Flow Transformer for Encrypted Traffic Classification. In Proceedings of the 28th ACM SIGKDD Conference on Knowledge Discovery and Data Mining, Washington, DC, USA, 14–18 August 2022; pp. 2576–2584.
73. Deshmukh, P.; Satyanarayana, G.S.R.; Majhi, S.; Sahoo, U.K.; Das, S.K. Swin transformer based vehicle detection in undisciplined traffic environment. *Expert Syst. Appl.* **2023**, *213*, 118992. [CrossRef]
74. Zhao, R.; Huang, Y.; Deng, X.; Xue, Z.; Li, J.; Huang, Z.; Wang, Y. Flow Transformer: A Novel Anonymity Network Traffic Classifier with Attention Mechanism. In Proceedings of the 2021 17th International Conference on Mobility, Sensing and Networking (MSN), Exeter, UK, 13–15 December 2021; pp. 223–230.
75. Lin, X.; Xiong, G.; Gou, G.; Li, Z.; Shi, J.; Yu, J. Et-bert: A contextualized datagram representation with pre-training transformers for encrypted traffic classification. In Proceedings of the ACM Web Conference 2022 Virtual Event, Lyon, France, 25–29 April 2022; pp. 633–642.
76. Schlette, D.; Caselli, M.; Pernul, G. A comparative study on cyber threat intelligence: The security incident response perspective. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 2525–2556. [CrossRef]
77. Killcrece, G.; Kossakowski, K.P.; Ruefle, R.; Zajicek, M. *State of the Practice of Computer Security Incident Response Teams (CSIRTs)*; Carnegie Mellon University, Software Engineering Institute: Pittsburgh, PA, USA, 2003.
78. Zhang, X.; Wang, Y.; Geng, G.; Yu, J. Delay-Optimized Multicast Tree Packing in Software-Defined Networks. *IEEE Trans. Serv. Comput.* **2023**, *16*, 261–275. [CrossRef]
79. Tøndel, I.A.; Line, M.B.; Jaatun, M.G. Information security incident management: Current practice as reported in the literature. *Comput. Secur.* **2014**, *45*, 42–57. [CrossRef]