symmetry

MDPI

Article

Real-Time Risk Detection Method and Protection Strategy for Intelligent Ship Network Security Based on Cloud Computing

Jian Guo [1,*] and Hua Guo [2]

[1] School of Management, Tianjin University of Technology, Tianjin 300384, China
[2] School of Electronics and Information Engineering, Tiangong University, Tianjin 300387, China; guohua@tiangong.edu.cn
* Correspondence: guojian@tjut.edu.cn

Abstract: When studying an unfamiliar system, we first look for the symmetry that the system has, so that we can make many predictions about the possible properties of the system. The symmetry in ship network security needs to maintain a stable state and maintain a constant state of ship network security. With the rapid development of network information technology, smart ships have become a new hot spot in the international shipping industry. The smart ships cybersecurity discussion is also at the top of the list in the maritime field. More and more shipping companies feel that their smart ship systems need to be upgraded and the main reason behind this is that the systems are maliciously attacked by cyber hackers. Therefore, it is extremely important to detect and protect the security of intelligent ship network systems in real time. The issue of network security has always accompanied the whole process of the development of the Internet. At the same time, with the development of Internet technology, network hacking attacks against the Internet have never stopped developing, and traditional ship network security risk detection and protection cannot achieve good results. After understanding the operation mode of intelligent ship networks, this paper deeply studied the characteristics of cloud computing technology and proposed a real-time risk detection method and protection strategy for intelligent ship network security based on cloud computing. This paper mainly used multi-sensor nodes to analyze data containing malicious attack information and implemented self-execution protection strategy generation nodes to intercept and protect from the attack, so as to achieve the purpose of maintaining the network security of intelligent ships. Through experiments, the virus intrusion detection and defense rate of the algorithm proposed in this paper was able to reach 85% to 95%, while the virus intrusion detection defense rate of the traditional intelligent ship network security protection algorithm was 55% to 65%. The detection rate of the algorithm proposed in this paper was able to reach 96.95% and the false positive rate was 2.56%. The detection rate of the traditional algorithm was only 70.76%, while the false positive rate reached 4.69%. All of the proposed algorithm's data were significantly better than that of traditional algorithms, which proved that the performance of cloud computing-based real-time risk detection and protection algorithms for intelligent ship network security was significantly better than that of traditional algorithms.

Keywords: security risk detection and protection; smart ship network; cloud computing; sensor nodes

check for updates

Citation: Guo, J.; Guo, H. Real-Time Risk Detection Method and Protection Strategy for Intelligent Ship Network Security Based on Cloud Computing. *Symmetry* **2023**, *15*, 988. https://doi.org/10.3390/sym15050988

Academic Editor: Achyut Shankar

Received: 7 March 2023
Revised: 30 March 2023
Accepted: 31 March 2023
Published: 27 April 2023

Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

1.1. Background Introduction

The expanding application scope of intelligent technology will also lead to an increasing number of various network security risks. It is necessary to develop a symmetrical and feasible network security architecture based on existing standards, continuously optimize top-level planning documents, and enhance the security of intelligent ship network systems. In response to this, it is necessary to develop a symmetrical planning plan for intelligent ship network security in accordance with national standard technology network security architecture content. The rapid development of information technology has also indirectly

driven all walks of life, including the shipping industry. The development of traditional shipbuilding and the shipping industry is limited due to a series of reasons such as long transportation time, uncertainty and danger during transportation, and severe weather influence. The emergence of smart ships has gradually changed this situation. The so-called smart ship is capable of obtaining the data of the ship itself and of the surrounding marine environment, as well as of the departure and arrival ports, through relevant information technology means so as to guide the operation of the ship intelligently. This not only makes the ship safer to drive, but also reduces transport time. At the same time, according to the weather conditions, preparatory plans are made in advance to save transportation costs. Therefore, the emergence of intelligent ships is undoubtedly the savior of the development of ships. However, the premise of realizing the intelligent ship is to ensure the real-time security of the network, otherwise it would face the risk of related information leakage. The occurrence of network paralysis is a test of the physical and psychological quality of the ship transporters, which affects the work efficiency and the normal operation of the ship. How to protect the security of the smart ship network from malicious attacks by network hackers? This requires the design of relevant algorithms to resist the maliciousness and attacks of viruses. The traditional algorithm, such as virus data protection software, can also resist some network virus attacks through the detection of existing virus attack forms. Once similar attacks are found, the system will automatically delete this kind of data to achieve the purpose of protection. However, with the continuous development of information technology, the viruses designed by network hackers are becoming more and more advanced. Traditional algorithms cannot resist the strong attacks of network hackers at all, so they are losing ground and cannot meet the needs of users. Therefore, this paper proposes an examination of intelligent ship network security detection and a protection algorithm based on cloud computing, so as to realize real-time detection and interception of viruses.

Current research on intelligent security prevention mainly includes: Meidan, Y. infected nine commercial Internet of Things (IoT) devices in the lab with the two of the best known IoT-based botnets Mirai and Bashlett viruses. The results of their evaluation showed that their proposed method detected their attacks accurately and instantly. This method is widely used by large enterprises and can indeed provide a series of solutions, but most of these firewalls have a high cost to use, so this is not recommended [1]. Amrita proposed a hybrid feature selection method for the intelligent lightweight Network Intrusion Detection System (NIDS)-Heterogeneous Ensemble of Intelligent Classifiers (HyFSA-HEIC), which aimed to classify anomalies of incoming traffic [2]. Mugabo, E. proposed a Merchant Category Code (MCC) intrusion detection method based on Support Vector Machine (SVM) and Information Gain (IG). The SVM classifier was used to classify the network data into normal behaviors and aggressive behaviors. Due to the presence of irrelevant and redundant features in the Knowledge Discovery and Data (KDD) mining data set, this method could detect malicious attacks with high accuracy and true positive rate, low false positive rate, and fast training [3]. Rais, H. M. proposed a new feature selection algorithm called dynamic ant colony system with three-level update feature selection. The method he proposed used different levels of pheromones to help ants find robust features. Anomaly-based detection methods could detect new attacks well [4]. The algorithms proposed in these studies can effectively detect and resist malicious attacks in network security, but the network security risks of smart ships are not studied enough. This research is based on cloud computing technology, intelligently controlling the ship network system through cloud computing, scanning the area with or which may have a Trojan virus in the network system, and eliminating the potential network security risks in the system.

1.2. Related Work

In the intelligent ship network, cloud computing technology can be used to realize the real-time monitoring of its security risks and formulate corresponding countermeasures. The main research and development focus of cloud computing technology is as follows: by

jointly optimizing unloading decisions, DuJ can reasonably allocate computing resources, transmission power, and radio-electronic measurement bandwidth to solve problems such as mixture and computing unloading cloud system, while improving application fairness and maximum tolerance delay [5]. Wang provides an experimental system capable of using a variety of online quality of service (QoS)-aware adaptive task assignment methods. He devised and compared three such methods, thus overcoming the problem that application features and workload vary widely and change with time [6]. Sheng, Z. proposed a new method to reduce the energy consumption of multimedia wireless sensor network (MWSN) processing application and meet certain completion time requirements; likewise, he proposed an energy-saving collaborative node selection strategy to provide a trade-off between fairness and energy consumption [7]. Li, Q. proposes an integrated approach to meet the cost of various service-level objects (SLOs). The method employs a three-tier resource controller using different analysis techniques, including feedback control theory, statistical machine learning, and system identification. Compared with Xen, we chose the core-based virtual machine (KVM) as the virtual machine (VM) monitor to implement the proposed method [8].

More and more attention has been paid to the network security of smart ships by shipping companies. In order to better meet the needs of users and protect the intelligent ship network from malicious attacks by hackers, cloud computing technology is used to perform corresponding algorithm calculations through sensor nodes and self-execute protection strategy generation nodes to screen and intercept network information.

2. Real-Time Detection Methods and Protection Strategies for the Network Security Risks of Smart Ships

The real-time detection method of intelligent ship network security risks is deeply combined with the symmetry concept, which is in line with high-quality research and has the characteristics of relevance to the subject. The structure of the traditional ship system network is generally static and deterministic, so it is only necessary to set up detection and interception at the edge of the ship network to effectively prevent malicious attacks by hackers. However, due to the dynamic, flexible, multi-tenant, and shared characteristics of cloud computing technology itself, the intelligent ship network based on cloud computing makes the boundary of the ship network no longer determined and ambiguity and multiple possibilities exist. Due to the complexity of the intelligent ship network, its fast and accurate protection has become a difficult point in the field of network security research. After fully considering the characteristics of intelligent ship network and cloud computing network, a new real-time detection method of ship network security risk is proposed, which can effectively achieve the effect of protecting intelligent ship network security [9].

At present, the shipping industry has recognized the risks that ship digitization and networking may pose, and the issue of ship network security has been widely discussed at the IMO conference in recent years. In June 2016, the Interim Guidelines for Maritime Network Risk Management was issued. No matter how malicious network attacks change, their essence is still data packets. Therefore, in order to intercept network attacks, it is necessary to obtain the data packets of malicious attacks and analyze them to decipher what network vulnerabilities it exploits and what are its attack methods. Therefore, it is necessary to set an algorithm at the ingress of the smart ship network to copy all network data and classify the copied data through a data analysis device, as well as finally set an algorithm to analyze the captured data packets.

In the environment of ship network security, the main goal of detecting intrusion viruses is to detect viruses in the ship's Internet data. Therefore, the main goal of intrusion virus detection is to obtain the ship's Internet data. This means that the collection process must expand the coverage of data as much as possible so as to fully monitor the marine network of ships and maintain their safety at sea, as well as to ensure their smooth navigation [10,11]. According to the characteristics of cloud computing technology and smart ships, this paper sets up the data collection and analysis architecture diagram of smart ships

under cloud computing technology as shown in Figure 1, which includes functions such as dynamic collection, activity query, system modeling, information monitoring, collection, and data analysis. Among them, according to the characteristics of cloud computing, the function of dynamically collecting information is used to build an intelligent ship network in the front-end part. The network architecture module integrates redirection and load balancing techniques to maximize system resource utilization, while data monitoring and behavior recording can centrally analyze and process information about threats [12].

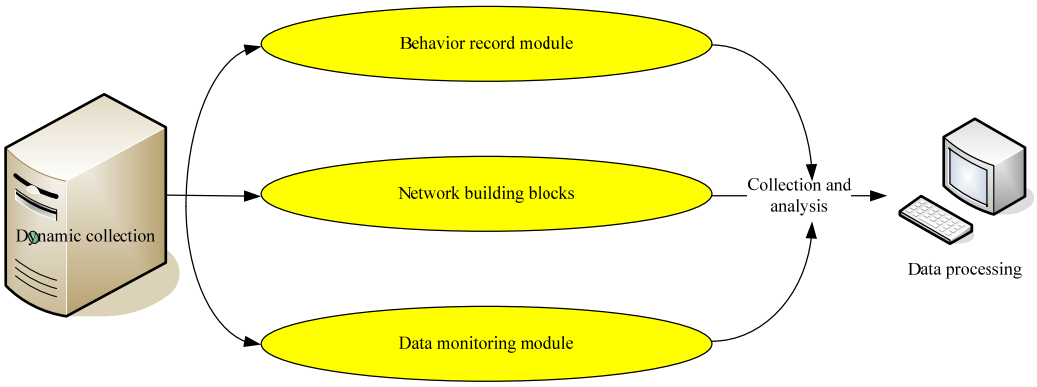

Figure 1. Data collection and analysis architecture diagram of smart ships under cloud computing technology.

In cloud computing, each virtual machine can be regarded as a node which can perform simple log analyses and processing and is also called a sensor node. Based on this, the running status of the current system can be sensed by running a lightweight system monitoring and alerting program. The program can be adjusted for each virtual machine and it can be optimized and adjusted appropriately according to the processing power of the virtual machine in which it resides [13,14]. For example, if the machine running the monitoring software is underperforming or under heavy load, the monitoring software can analyze only basic system information. Although only the basic system information can be analyzed, when the supervision of the monitoring software is too low, the software will obtain the corresponding information in other ways to ensure the information acquisition rate. If the operating host is lightly loaded, advanced system information can be logged. In addition to analyzing and reporting the system status, sensor nodes can also trigger immune processing based on protection strategies. According to the protection information sent by the generation node of the protection strategy, the intelligent ship network immune processing module can trigger the relevant protection mechanism and intercept malicious network virus attacks so as to protect the intelligent ship network system from damage.

In addition to sensor nodes, the cloud computing-based intelligent ship network security protection system also has another self-executing protection strategy generation node that detects monitoring data and forms protection strategies, as shown in Figure 2. Its main function is to analyze the aggregated and collected alarm data and start the protection mechanism by matching the corresponding protection strategy for the data with potential risk threats. The self-enforcing protection strategy generation node is a key part of the entire logical network, and the node includes two parts: business processing and security response. Therefore, the security response node can be upgraded to become a self-executing protection strategy generation node, and the process is simple and convenient [15,16]. Figure 2 shows the relationship between the self-executing protection strategy generation node and the sensor node. The self-enforcing protection strategy generation node is composed of several sensor nodes connected, but some sensor nodes cannot directly connect to the self-enforcing protection strategy generation node. Therefore, the data of these sensor nodes should be forwarded and connected by other sensor nodes so as to achieve the purpose of real-time risk detection and protection of the intelligent ship network.

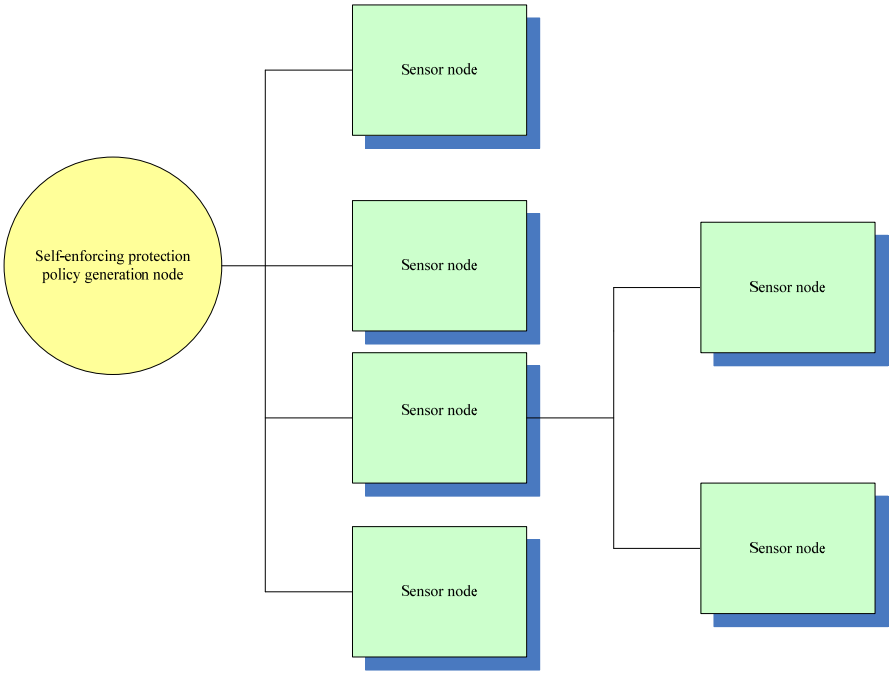

Figure 2. The relationship between the self-executing protection strategy generation node and the sensor nodes.

Each sensor node has a dedicated algorithm that can collect and analyze data on the state of the intelligent ship network system. It exists and runs in the form of a service in the ship's virtual machine system, which has super high authority that cannot be terminated. Sensor nodes can collect data through polling mode and event-triggered mode, and finally achieve the effect of triggering risk assessment procedures. Among them, in the polling mode, the program would scan and collect the key information of the system every specific time. This time can be dynamically adjusted based on the actual situation of the virtual machine load pressure and processing power. However, it must be noted that this time must not exceed the threshold, otherwise it would not be able to respond immediately to cyber risks; under the event-triggered model, smart ship network users can set several triggering events. When the threshold is exceeded, the intelligent ship network can judge that the current situation requires emergency measures [17]. The specific process of intelligent ship network risk monitoring based on cloud computing technology is: basic information such as processes, registered users, and ports are scanned to determine whether the current load reaches the threshold. If the threshold is reached, the risk assessment procedure is triggered; if not, it continues with advanced scanning methods such as memory and packets.

After completing the risk detection step, the intelligent ship network security system would initially analyze the risk to decide whether to report to the higher-level risk detection node, which is called data preprocessing. The reason for data preprocessing is that the self-enforcing protection policy generation node generally needs dozens or even hundreds of virtual machines to reach a safe state. If it is directly reported to the superior node without data preprocessing, the self-executing protection strategy generation node would affect the final protection result due to excessive pressure [18,19]. The basic flowchart of data preprocessing is shown in Figure 3. The first step is to merge data and remove duplicate data at the same time. The data generated by the polling mode and the event-triggered mode mentioned above are both due to the same risk. These two data can be merged to reduce the subsequent processing pressure. The second step is data filtering: the data obtained in the risk detection stage may be triggered by some unexpected situations which are not real risk threats. For example, when too many people access the server at the same time, the load of the processor would be too high. When the amount of access is reduced, it can be restored to the normal state. Therefore, such data information needs

to be filtered and processed. The last step is data compression: it cannot be ignored that data compression can reduce the pressure of network compression and correspondingly increase the consumption of the processor. Therefore, whether the data is compressed or not depends on the actual operation of the virtual machine. If the load of the processor is too high, the compression algorithm may not be used or only a simple data compression algorithm may be used.

Figure 3. The basic flowchart of data preprocessing.

The self-executing protection strategy generation node summarizes the data obtained after detection by each sensor node and then judges potential risks. Its number would be adjusted with the actual number of virtual machines in the smart ship network, which is uncertain. The self-executing protection strategy generation node and sensor nodes run together in the smart ship network, which also makes the dynamic adjustment of risk protection nodes very simple. It only needs to package the operating environment of all nodes and create a virtual machine image to achieve the effect [20].

As shown in Figure 4, the real-time processing process of intelligent ship network risk protection is followed by risk classification, risk summary rule generation, and rule issuance. Among them, risk classification consists of classifying the data transmitted by the sensor nodes according to the security type, and dividing the risks into several major categories: malware, vulnerability attack, personal information protection leakage, and network telecommunication fraud. After risk classification, interference can be reduced and the accuracy of risk identification of the intelligent ship network system can be improved; risk aggregation is to combine and summarize the information that the same attack causes more responses to sensor nodes. For example, a network attacker's attack on a homepage in the smart ship network caused the homepage server to stop running. Since most of the homepage part of the network is operated by the front-end load balancing and the back-end server cluster, the back-end server would issue the same alarm information when it is maliciously attacked [21]. Therefore, the same sensor nodes can be aggregated to simplify the workflow and improve the efficiency of risk identification;. Rule generation is a rule set formed by the intelligent ship network system through relevant definitions, which contains the processing methods for different risk types. However, it should be noted that due to the vulnerability of the intelligent ship system itself, when network attackers use this to launch attacks, protection software cannot be used to intercept these attacks. At this time, the intelligent ship network system should immediately prevent this part of the virtual machine from accessing the network to avoid the avalanche effect. The last part is the rule distribution part: the distribution path needs to be selected first and then the policy generated by the protection node can be sent to the protection deployment node. The selection of the delivery path algorithm is also very important because the receiver of the protection strategy may be one sensor or multiple sensors. This paper proposes a cloud computing-based intelligent ship network protection strategy system using Dijkstra's algorithm for emergency tasks and a breadth-first algorithm for broadcast tasks. Dijkstra's algorithm (Dijkstra) was proposed by Dutch computer scientist Dijkstra in 1959, so it is also called Dijkstra's algorithm. The shortest path algorithm from one vertex to the other vertices solves the shortest path problem in the power graph. The main feature of Dijkstra's algorithm is that it starts from the starting point, adopts the greedy algorithm strategy, and traverses the adjacency node of the closest and unvisited vertex to the starting point every time until it extends to the end point. There are relatively few attacked points at the beginning of the malicious attack. At this time, Dijkstra's algorithm has obvious advantages, which can quickly protect the virtual machine maliciously attacked by hackers and prevent the attack from spreading. By using Dijkstra's algorithm, the strategy generated by the

self-executing protection strategy generation node can be sent to the maliciously attacked virtual machine at the fastest speed, so as to complete the interception task and ensure the normal operation of the intelligent ship network system. In the case that the breadth of the hacking attack is relatively large, the breadth-first algorithm needs to be used. For example, when the initial protection strategy fails to intercept network attacks and a larger area of failure occurs, the intelligent ship network protection system would further generate strategies. At this time, the protection policy node needs to send more virtual machines, so the breadth-first algorithm is used to ensure the delivery speed. The overall process of the real-time risk detection and protection strategy of an intelligent ship network system is shown in Figure 5 [22].

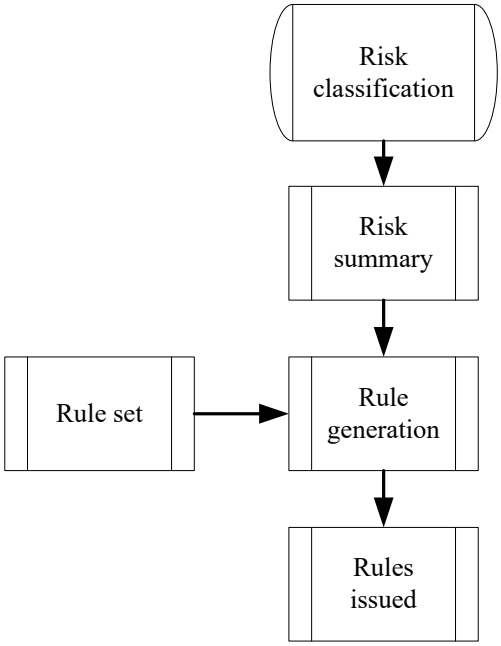

Figure 4. Risk-handling process.

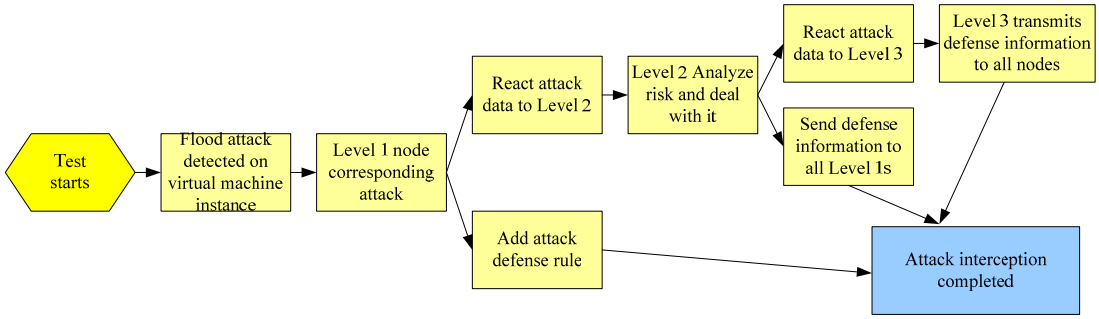

Figure 5. The overall process of the real-time risk detection and protection strategy of an intelligent ship network system.

In this paper, some relevant algorithms for real-time risk detection and protection strategies of an intelligent ship network based on cloud computing are selected as follows:

$$p_{a(m)} = \sum_{m_b : b \in N_a} \left[\prod_{b \in N_a} p_{a \leftarrow b(m_a)} \right] \sigma(\mathrm{m} - 1, \sum_{b \in N_a} \mathrm{m_b}), \quad (1)$$

where $p_{a(m)}$ is the probability that the a-th smart ship network sensor node belongs to the set of m nodes.

$$\sigma(i, j) = \begin{cases} 1, i - j = 0 \\ 0, i - j \neq 0' \end{cases} \quad (2)$$

where $\sigma(i, j)$ is the Kronecker function.

$$q_{a(n)} = \sum_{m=1}^{\infty} p_{a(m)} n^m, \tag{3}$$

where $q_{a(n)}$ is the probability generation function of sensor nodes of the intelligent ship network system.

$$q_{a(n)} = \sum_{m=1}^{\infty} n^m \sum_{m_b : b \in N_a} \left[\prod_{b \in N_a} p_{a \leftarrow b(m_a)} \right] \sigma(\mathrm{m} - 1, \sum_{b \in N_a} \mathrm{m_b}) \tag{4}$$

The previous formula is simplified to get:

$$q_{a(n)} = \mathrm{n} \prod_{b \in N_a} \sum_{m_b=0}^{\infty} p_{a \leftarrow b(m_b)} q^{p_b} \tag{5}$$

Let the formulas be:

$$Z_{a \leftarrow b(n)} = \sum_{m_b=0}^{\infty} p_{a \leftarrow b(m_b)} q^{p_b}, \tag{6}$$

$$\prod_{b \in N_a} z_{a \leftarrow b(n)} = \sum_{m=0}^{\infty} p_{a \leftarrow b(m)} q^m, \text{ and} \tag{7}$$

$$k_{a \leftarrow b} = (1 - \mu)^2 R_{amu}(b), \tag{8}$$

where $k_{a \leftarrow b}$ is the probability of the existence of edges between nodes a and b; μ-nodes are initially removed.

$$p_{a \leftarrow b(m)} = k_{a \leftarrow b} \sum_{m_x : x \in N_{b \setminus a}} \left[\prod_{x \in N_{b \setminus a}} p_{b \leftarrow x(m_x)} \right] \sigma(\mathrm{m} - 1, \sum_{x \in N_{b \setminus a}} m_x) \tag{9}$$

where $N_{b \setminus a}$ are child nodes in sensor node b, which excluded sensor node a.

$$k'_{a \leftarrow b} = (1 - \mu)^2 (1 - R_{amu}(b)) (1 - R_{b \in T}), \tag{10}$$

where $k'_{a \leftarrow b}$ is the key protection node of the smart ship network.

$$Z_{a \leftarrow b(n)} = (1 - k_{a \leftarrow b} + k_{a \leftarrow b} \prod_{x \in N_{b \setminus a}}) Z_{b \leftarrow x(1)}, \tag{11}$$

where $Z_{a \leftarrow b(n)}$ is the largest connected node scale of the intelligent ship network.

The maximum connection node scale of the intelligent ship network. The above is the algorithm formula of the network protection system. Through it, a complete intelligent ship network protection system can be built.

3. Experiment of Real-Time Detection and Protection of the Intelligent Ship Network Security Risk

Ship network security as the whole rear guarantee, the ship must always be in an absolute state of safety to ensure its normal operation [23,24]. For example, maritime container transport ships attach great importance to the security protection of the ship network system due to the relatively high value of their cargo ships. A dynamic network is adopted to protect network security [25,26]. In order to test whether the intelligent ship network real-time detection and protection strategy proposed in this paper can achieve the expected effect, relevant experiments were carried out after the algorithm was formed and the resulting data were statistically analyzed. The experimental results are as follows:

By using python to input the detection data set into the detection algorithm every 1 min, the algorithm testing for detecting vertical port scanning events and the algorithm testing for detecting horizontal port scanning events were performed in turn, and the obtained results are shown in Figures 6 and 7. Both the number of detected vertical port scan events and the number of horizontal port scan events decreased as the detected data

set increased, which is in line with expectations. In practice, the detection data set can be adjusted according to the actual needs of the intelligent ship network users.

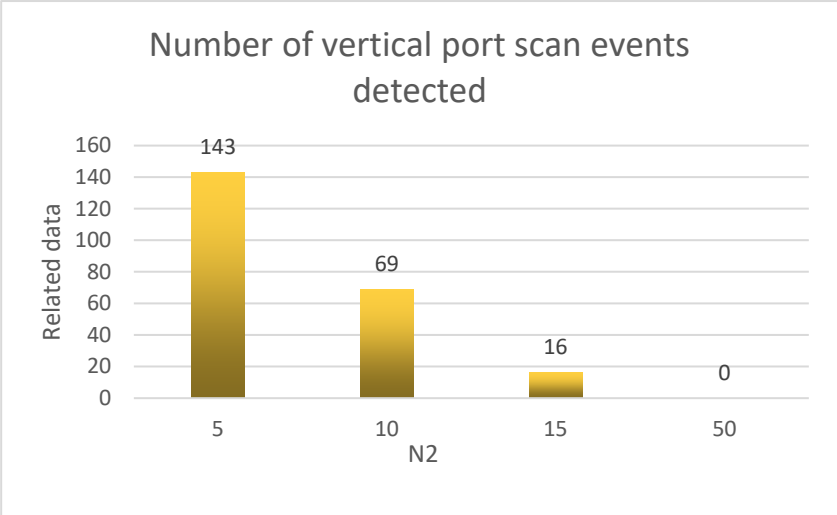

Figure 6. Vertical scan event detection results.

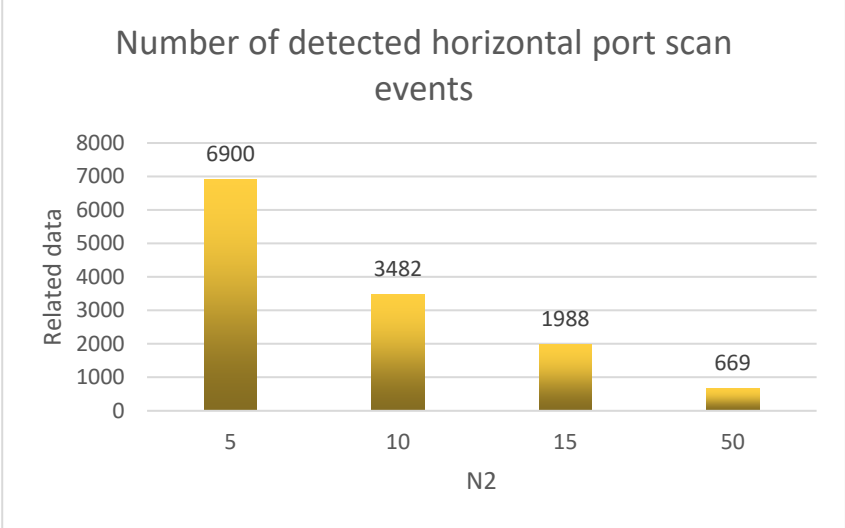

Figure 7. Horizontal scan event detection results.

In the process of shipping, ships are confronted with security challenges all the time, and all the network supply chain systems on board are confronted with network security risks such as virus intrusion [27,28]. We tested the influence of the real-time detection and protection strategy on virus invasion, and analyzed the performance of the real-time detection and protection strategy under this algorithm. In the experiment, the experimental group and the traditional intelligent ship network security protection control group were established, the number of invading viruses was set to 100, and the effective defense of virus invasion under the two methods was analyzed. In order to make the data realistic, a common virus was randomly selected for experimental testing and the results are shown in Figure 8 and Table 1. The algorithm proposed in this paper was able to detect and defend against 85 cyber virus attacks in the first 10 experiments, while the traditional intelligent ship network security protection algorithm was only able to detect and defend against 56 cyber virus attacks on average. With the increase of experiment number, the algorithm proposed in this paper was able to generally detect 85 to 95 (the highest was even able to reach 98), while the traditional intelligent ship network security protection algorithm was

able to generally detect 55 to 65 (the highest was only 74). That is to say, the virus intrusion detection and defense rate of the proposed algorithm can reach 85–95% efficacy, while the virus intrusion detection and defense rate of the traditional intelligent ship network security protection algorithm can reach 55–65% efficacy. Compared with the latter, the proposed algorithm improved the effective defense rate by nearly 30%, which indicates that the algorithm has a good real-time risk detection and protection effect.

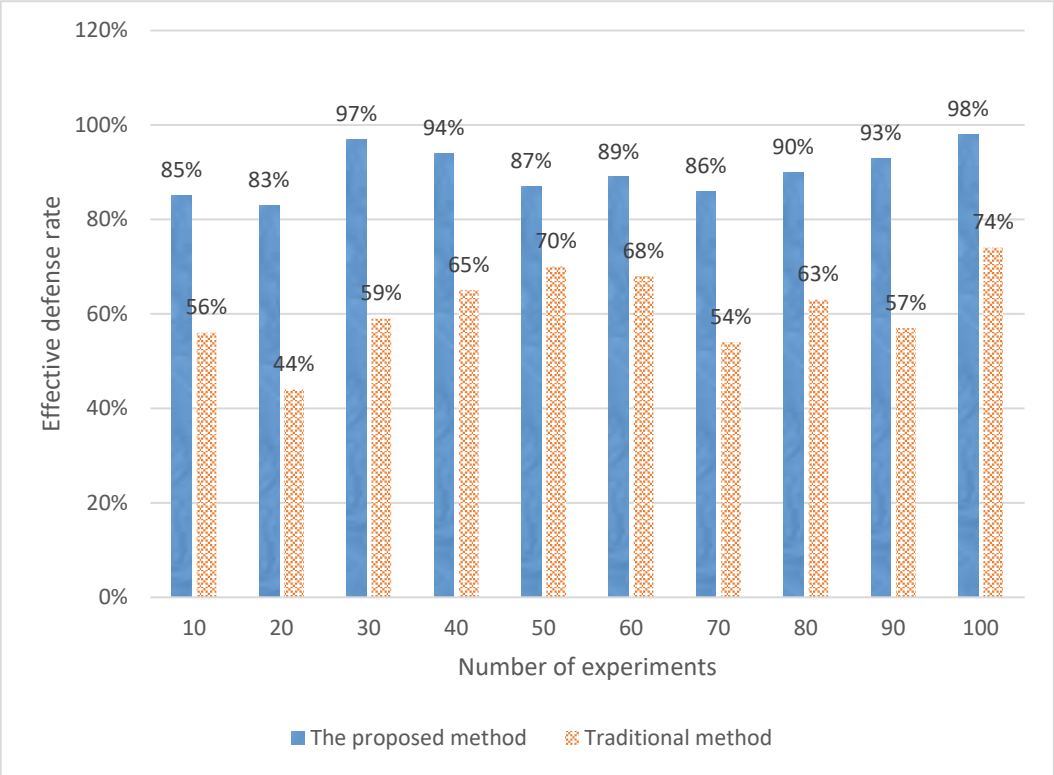

Figure 8. Effective defense rate against virus intrusion.

Table 1. The experimental results of the proposed algorithm.

Protocol Type	Traffic Control Panel	UDP	Network Control Message Protocol	Average Value
Total number of trials	6879	5264	4825	5656
Invasion times	2653	2784	1652	2363
Number of test bars	2594	2720	1560	2291
Doctor (%)	97.78	97.70	94.43	96.95
False alarms	174	138	124	145
Fr (%)	2.53	2.62	2.57	2.56

Next, a wider range of detection tests were carried out to compare and analyze the proposed algorithm and the traditional algorithm, and the results obtained are shown in Table 2. It can be seen that there were 6879 test TCPs in total, of which 2653 had virus information. Intelligent ships have autonomous detection capabilities and can conduct intelligent detection of their own network security through system algorithms [29]. The algorithm proposed in this paper was able to detect 2594 and the number of false warnings was 174, which means that the detection rate reached 97.78% and the false positive rate was 2.53%. The traditional algorithm was able to detect 1988 and the number of false warnings was 324. That is to say, the detection rate was 74.93% and the false positive rate was 4.71%. A total of 5264 UDPs were tested, of which 2784 had virus information. The algorithm proposed in this paper was able to detect 2720 and the number of false warnings was 138,

which means that the detection rate reached 97.70% and the false positive rate was 2.62%. The traditional algorithm was able to detect 1890 and the number of false warnings was 284. That is to say, the detection rate was 67.89% and the false positive rate was 5.40%. A total of 4825 ICMPs were tested, of which 1652 had virus information. The algorithm proposed in this paper was able to detect 1560 and the number of false warnings was 124, which means that the detection rate reached 94.43% and the false positive rate was 2.57%. The traditional algorithm was able to detect 1137 and the number of false warnings was 187. That is to say, the detection rate was 68.83% and the false positive rate was 3.88%. On average, the detection rate of the algorithm proposed in this paper was able to reach 96.95% and the false alarm rate was 2.56%. Meanwhile, the detection rate of the traditional algorithm was only 70.76% and the false alarm rate reached 4.69%. The detection rate of the algorithm proposed in this paper was 26.19% higher than that of the traditional algorithm, and the false alarm rate was 2.13% lower than that of the traditional algorithm. Therefore, it can be clearly seen from the experimental results that the real-time detection method of the intelligent ship network based on cloud computing is superior to the traditional algorithm in terms of detection rate and false alarm rate. Although there are still false positives, the scale of malicious attacks on smart ship networks in reality is far from the number in the experiment. Therefore, the algorithm proposed in this paper can fully meet the security protection requirements of the intelligent ship network system.

Table 2. Experimental results of conventional algorithms.

Protocol Type	Traffic Control Panel	UDP	Network Control Message Protocol	Average Value
Total number of trials	6879	5264	4825	5656
Invasion times	2653	2784	1652	2363
Number of test bars	1988	1890	1137	1672
Doctor (%)	74.93	67.89	68.83	70.76
False alarm	324	284	187	265
Fr (%)	4.71	5.40	3.88	4.69

In terms of the accuracy of risk identification of the ship intelligent network system, this paper also analyzed the corresponding data of the proposed algorithm. Table 3 is the analysis table of risk identification accuracy data of the intelligent network system:

Table 3. Risk identification accuracy data analysis table of the intelligent network system.

	Intelligent Network System	Traditional Network System	Difference Value
Data 1	97%	60%	37%
Data 2	99%	70%	29%
Data 3	100%	70%	30%
Data 4	99%	68%	31%
Data 5	100%	70%	30%

In terms of the accuracy of risk identification, the accuracy of the traditional system is slightly worse, mostly hovering between 60% and 70%. The accuracy of risk identification is 70% at the highest, 60% at the lowest, and the accuracy difference is 10%. Meanwhile, the recognition accuracy rate of the intelligent network system is 100% at the highest, 97% at the lowest, with a difference of only 3%. There is not only a difference in the accuracy range between the two, but also a large difference in the overall accuracy range. The reason for this situation is mainly because, in terms of data processing, the traditional system recognizes and detects all data in turn. Therefore, some irrelevant data will also be detected and identified, which leads to a decline in accuracy. The intelligent system will conduct intelligent screening of the data that has nothing to do with the edge and only detect the undetected data. The previously detected data will not be tested again, so as to improve

the accuracy of data risk identification. Therefore, in terms of the accuracy of system risk identification, the intelligent network system is better than the traditional system.

4. Research Results and Significance Summary

The research results of the intelligent ship network security system show that compared with the traditional system, the proposed system can protect the ship network security more effectively and prevent network attacks and data leakage. Therefore, the design of this system is of certain value and significance. The system uses a variety of security technologies, including intrusion detection and data encryption, to identify and respond to cyber threats inside and outside the ship in a timely manner. The key points of the intelligent ship network security system are to encrypt important data, prevent sensitive information from leaking, establish a security monitoring system, discover and deal with security incidents in time, and have an emergency response mechanism to ensure the ship's network security. The significance of this research lies in improving the level of ship network security and ensuring the safe operation of ships and the safe transportation of goods. With the deepening application of intelligent technology in the shipping industry, more and more attention will be paid to the problem of ship network security. The research results of the intelligent ship network security system provide feasible solutions for ship network security and provide strong support for the digital transformation of the ship industry.

5. Conclusions

In order to ensure the network security of smart ships, this paper provided a monitoring and defense technology method for the network security of smart ships based on cloud computing technology. Its advantage was that it had super-large-scale processing capabilities and the authenticity of the calculation results was also quite high. When the proposed method was finally completed, this paper also conducted relevant experiments on its virus detection function and compared it with the traditional method. The large number of experimental data showed that the network security of intelligent ships is more comprehensive than that of traditional ships. The experimental conclusion also proved that the virus detection success rate and defense success rate of the algorithm proposed in this paper were much higher than those of the traditional method and the probability of false positives was also lower than that of the traditional method. This showed that the method in this paper was quite efficient in ensuring the network security of smart ships. However, there are still many shortcomings: for example, the number of trials is relatively small; the conclusions drawn may have some deviations; the types of virus samples used for testing are not complete; and there may be blind spots for detection and protection. The application of smart ships would bring new vitality to the shipping industry, and the issue of network security is also a key research area for the development of information technology. It is also hoped that more people would participate in network security protection research in the future to maintain the smooth operation of network security.

Author Contributions: J.G. and H.G. designed and performed the experiment and prepared this manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data that support the findings of this study are available from the corresponding author upon reasonable request.

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

References

1. Meidan, Y.; Bohadana, M.; Mathov, Y. N-BaIoT: Network-based Detection of IoT Botnet Attacks Using Deep Autoencoders. *IEEE Pervasive Comput.* **2018**, *17*, 12–22. [CrossRef]
2. Amrita, K.K.R. A Hybrid Intrusion Detection System: Integrating Hybrid Feature Selection Approach with Heterogeneous Ensemble of Intelligent Classifiers. *Int. J. Netw. Secur.* **2018**, *20*, 40–53.
3. Mugabo, E.; Zhang, Q.Y. Intrusion Detection Method Based on Support Vector Machine and Information Gain for Mobile Cloud Computing. *Int. J. Netw. Secur.* **2019**, *22*, 231–241.
4. Rais, H.M.; Mehmood, T. Dynamic Ant Colony System with Three Level Update Feature Selection for Intrusion Detection. *Int. J. Netw. Secur.* **2018**, *20*, 184–192.
5. Du, J.; Zhao, L.; Jie, F. Computation Offloading and Resource Allocation in Mixed Fog/Cloud Computing Systems with Min-Max Fairness Guarantee. *IEEE Trans. Commun.* **2018**, *66*, 1594–1608. [CrossRef]
6. Wang, L.; Gelenbe, E. Adaptive Dispatching of Tasks in the Cloud. *IEEE Trans. Cloud Comput.* **2018**, *6*, 33–45. [CrossRef]
7. Sheng, Z.; Mahapatra, C.; Leung, V. Energy Efficient Cooperative Computing in Mobile Wireless Sensor Networks. *IEEE Trans. Cloud Comput.* **2018**, *6*, 114–126. [CrossRef]
8. Li, Q.; Hao, Q.F.; Xiao, L.M. An Integrated Approach to Automatic Management of Virtualized Resources in Cloud Environments. *Comput. J.* **2018**, *54*, 905–919. [CrossRef]
9. Liu, X.F.; Zhan, Z.H.; Deng, J.D.; Li, Y.; Gu, T.; Zhang, J. An Energy Efficient Ant Colony System for Virtual Machine Placement in Cloud Computing. *IEEE Trans. Evol. Comput.* **2018**, *22*, 113–128. [CrossRef]
10. Rajiv, R.; Omer, R.; Surya, N. The Next Grand Challenges: Integrating the Internet of Things and Data Science. *IEEE Cloud Comput.* **2018**, *5*, 12–26.
11. Ning, J.; Cao, Z.; Dong, X. Auditable σ -Time Outsourced Attribute-Based Encryption for Access Control in Cloud Computing. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 94–105. [CrossRef]
12. Lee, E.S.; Park, S.H. A Legislative Study for strengthening of Ship Cyber Security. *Marit. Law Rev.* **2021**, *33*, 227–254. [CrossRef]
13. Lee, E.; Ahn, Y.J.; Park, S.H. A Study on the Development of a Training Course for Ship Cyber Security Officers. *J. Korean Soc. Mar. Environ. Saf.* **2020**, *26*, 830–837. [CrossRef]
14. Dogan, D. The importance of cyber security in Turkey's shipping industry. *Port Eng. Manag.* **2019**, *38*, 33.
15. Forbes, L. The global maritime industry remains unprepared for future cybersecurity challenges. *Shipbuild. Ind.* **2018**, *12*, 42–44.
16. Sandhu, A.K. Big Data with Cloud Computing: Discussions and Challenges. *Big Data Min. Anal.* **2022**, *5*, 32–40. [CrossRef]
17. Darwesh, A.; Rahimi, M.; Hosseinzadeh, M. Toward the efficient service selection approaches in cloud computing. *Kybernetes* **2022**, *51*, 1388–1412.
18. Ashammakhi, N.; Unluturk, B.D.; Kaarela, O. The Cells and the Implant Interact With the Biological System Via the Internet and Cloud Computing as the New Mediator. *J. Craniofacial Surg.* **2021**, *32*, 1655–1657. [CrossRef]
19. Dan, H. Ensuring Cybersecurity in Shipping: Reference to Estonian Shipowners. *Trans. Nav. Int. J. Mar. Navig. Saf. Sea Transp.* **2020**, *14*, 271–278.
20. Bakar, N.; Ibrahim, R.; Amron, M.T. Cloud computing acceptance among public sector employees. *TELKOMNIKA Telecommun. Comput. Electron. Control* **2021**, *19*, 126–135.
21. Nayar, K.B.; Kumar, V. Cost benefit analysis of cloud computing in education. *Int. J. Bus. Inf. Syst.* **2018**, *27*, 205.
22. Kumar, N.; Chilamkurti, N.; Zeadally, S. Achieving Quality of Service (QoS) Using Resource Allocation and Adaptive Scheduling in Cloud Computing with Grid Support. *Comput. J.* **2018**, *57*, 281–290. [CrossRef]
23. Roy, K.; Chaudhuri, S.S.; Pramanik, S.; Banerjee, S. Deep Neural Network Based Detection and Segmentation of Ships for Maritime Surveillance. *Comput. Syst. Sci. Eng.* **2023**, *44*, 647–662. [CrossRef]
24. Yasir, M.; Jianhua, W.; Mingming, X.; Hui, S.; Zhe, Z.; Shanwei, L.; Colak, A.T.I.; Hossain, M.S. Ship detection based on deep learning using SAR imagery: A systematic literature review. *Soft Comput.* **2023**, *27*, 63–84. [CrossRef]
25. Nguyen, S.; Chen, P.S.L.; Du, Y. Container shipping operational risks: An overview of assessment and analysis. *Marit. Policy Manag.* **2022**, *49*, 279–299. [CrossRef]
26. Maskooki, A.; Deb, K.; Kallio, M. A customized genetic algorithm for bi-objective routing in a dynamic network. *Eur. J. Oper. Res.* **2022**, *297*, 615–629. [CrossRef]
27. Kim, T.E.; Perera, L.P.; Sollid, M.P.; Batalden, B.M.; Sydnes, A. K Safety challenges related to autonomous ships in mixed navigational environments. *WMU J. Marit. Aff.* **2022**, *21*, 141–159. [CrossRef]
28. Hunaid, M.; Bhurgri, A.A.; Shaikh, A. Supply Chain Visibility in Leading Organizations of the Shipping Industry: Supply Chain in Shipping Industry. *South Asian J. Soc. Rev.* **2022**, *1*, 8–20. [CrossRef]
29. Munim, Z.H.; Saha, R.; Schøyen, H.; Ng, A.K.; Notteboom, T.E. Autonomous ships for container shipping in the Arctic routes. *J. Mar. Sci. Technol.* **2022**, *17*, 320–334. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.