Hindawi
Security and Communication Networks
Volume 2023, Article ID 9762641, 1 page
https://doi.org/10.1155/2023/9762641

Retraction

Retracted: Research on Network Security Situational Awareness Based on Crawler Algorithm

Security and Communication Networks

Received 10 October 2023; Accepted 10 October 2023; Published 11 October 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] X. Wu, D. Wei, B. P. Vasgi, A. K. Oleiwi, S. L. Bangare, and E. Asenso, "Research on Network Security Situational Awareness Based on Crawler Algorithm," *Security and Communication Networks*, vol. 2022, Article ID 3639174, 9 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 3639174, 9 pages
https://doi.org/10.1155/2022/3639174

Research Article

Research on Network Security Situational Awareness Based on Crawler Algorithm

Xu Wu,[1] **Dezhi Wei**,[2] **Bharati P. Vasgi**,[3] **Ahmed Kareem Oleiwi**,[4] **Sunil L. Bangare**,[5] **and Evans Asenso**[6]

[1]*Laboratory Management Center, Chengyi College, Jimei University, Xiamen, Fujian 361021, China*
[2]*Department of Information Engineering, Chengyi College, Jimei University, Xiamen, Fujian 361021, China*
[3]*Department of Information Technology, Marathwada Mitra Mandal's College of Engineering, Pune, India*
[4]*Department of Computer Technical Engineering, The Islamic University, Najaf 54001, Iraq*
[5]*Department of Information Technology, Sinhgad Academy of Engineering, Savitribai Phule Pune University, Pune, India*
[6]*Department of Agricultural Engineering, School of Engineering Sciences, University of Ghana, Accra, Ghana*

Correspondence should be addressed to Dezhi Wei; weidezhi8@126.com and Evans Asenso; easenso@ug.edu.gh

Received 10 May 2022; Revised 13 June 2022; Accepted 22 June 2022; Published 20 July 2022

Academic Editor: Mukesh Soni

Network security situation awareness is a critical basis for security solutions because it displays the target system's security state by assessing actual or possible cyber-attacks in the target system. Aiming at the security and stability of global information flow, this paper studies the perception and measurement of the overall situation of network security. Through the Scrappy web crawler framework, data were collected from several Zhiming network security event websites, and based on the vulnerability database of China Computer Network Intrusion Prevention Center, the network security event database was designed and established, which enriched the data of situational awareness research. This study investigates the analysis and processing of network security events, a crucial parameter in the stage of security insight and perception, and builds and implements a text-based network security event analysis tool. By designing a network security event analysis tool based on text processing, the data cleaning of network security time text information is completed, and a set of network security event processing solutions with high applicability and comprehensiveness are formed. Statistical experimental results show that the network security event database built based on the crawler algorithm contains 43,848 pieces of data, which increases the capacity by 12.79% and 29.33% compared with the traditional algorithm, and reduces the reading time by 63.5% and 87.2%.

1. Introduction

The use of the global Internet has grown exponentially, bringing new ways of transacting, communicating, learning, and socializing to everyday life. At the same time, the Internet has penetrated into the fields of economy, politics, transportation, education, agriculture, etc., playing an increasingly important role in different fields. According to the 2018 Internet Statistics Report [1] by the China Internet Network Information Center (CNNIC), the number of Internet users in China has reached 829 million, with 56.53 million new Internet users throughout the year, and the Internet penetration rate is 59.6%, compared with the same period in 2017, an increase of 3.8%. But at the same time, networked systems have gradually become the preferred target of organized crime groups. Unfortunately, the overall defense capabilities of current cyber systems are still in their infancy. Cyber security difficulties can range from minor issues such as out-of-date software to major issues such as a lack of leadership backing. The number of Internet-connected "smart" devices in both homes and businesses is increasing. The problem is that not all of these smart devices provide proper protection, allowing intruders to hijack systems and get access to business networks. With the popularization and promotion of network technology, the following severe situation of network security has become

difficult to ignore. The analysis methodology can extract analytically valuable security events from multi-source and heterogeneous huge raw data, and then discover security concerns, prospective threats, and unknown assaults. As there are different types of encryption, there are numerous means for attackers to transmit encrypted threats. Phishing, sensitive information theft, DOS attacks, ransomware, DDoS assaults, masquerading, pattern matching, and other network security threats are continually evolving. The scope of network security threats is constantly expanding, the research content of network security is also constantly enriched, and the network security situation and challenges are becoming more and more severe [2, 3].

With the increasing importance of cyberspace safety, more attention is being paid to cyber security stress detection research and applications (NSSA). The research decomposes an independent assault behavior into several separate time stages during the process of continuous evolution of the NSSA system, such as the IKC multi-stage attack model. NSSA realizes behavior identification, knowledge of purpose, and effect evaluation of diverse network operations in order to make suitable security response options. The occurrence of one network security event may influence the later creation of other network security events, demonstrating a tendency of chain evolution and increasing the complexity of network security events. NSSA realizes behavior identification, purpose understanding, and effect evaluation of various network operations to allow appropriate security response decisions [4, 5]. Network security events are both intrinsically related and affect each other [6]. Situational awareness can represent the overall condition of cyber security in real time and predict network security growth. The application of big data technology opens up new avenues for big network security spatial awareness research [7, 8]. The occurrence of one network security event may affect the subsequent development of different network security events, showing a trend of chain evolution, making the nature of network security events more complex. For complex networks, the longer the duration, the greater the impact and harm on work life. The evolution law of network security events includes not only the evolution law of a single network security event, but also the law of chain evolution between network security events. Identifying and understanding these evolution laws is very important for the analysis and perception of network security situation, a complete set of cyberspace security situational awareness solutions is shown in Figure 1. Figure 1 shows the schematic diagram representing security awareness solution. The platform will provide great convenience and has strong applicability; at the same time, it can also clearly present the internal connection of network security events.

This paper mainly studies the analysis and processing of network security events, an important parameter in the stage of awareness and understanding of security situation, and designs and implements a network security event analysis tool based on text processing. A hypernetwork-based network security event chain evolution model, based on the established network security database, verifies the effectiveness and practicability of the tools and models. The article presents a comprehensive introduction to the topic of network security situational awareness, with the goal of providing useful guidance for comprehending related ideas, encouraging their use in practice, and implementing large-scale network development. The data cleaning of network security time text information is finished by building a network security event analysis tool based on text processing, and a set of network security event processing solutions with high applicability and comprehensiveness is established.

The previous section is the introduction to the paper. Section 2 is the literature survey done related to the work done in the field of security. Research methodology has been discussed in section 3. Section 4 is the results analysis based on major findings. Conclusion of the paper has been covered in section 5.

2. Literature Review

Situational awareness can forecast network security growth by representing the complete state of cyber security in real time. Massive data technology application gives up new opportunities for big network security spatial awareness study. The network security event evolution law comprises not only the development rule of a single network security event, but also the law of chain evolution between network security events. References [9, 10] summarize that, by analyzing network security and recognizing anomalous events in the networks, one could anticipate the future security condition and prevent aberrant feedback. Big data-based network security situational awareness can aid in the resolution of increasingly complicated networking security concerns. With the growth of the Internet and global information, the encryption of the data is at risk threats that employ encryption to avoid detection and are known as encrypted threats. Malware, espionage, spear-phishing, zero-day, security breaches, malicious websites, and other attack types are among them. There are variety of techniques for attackers to communicate encrypted threats, just as there are numerous forms of encryption. The concept of situational awareness was first proposed by [11]; situational awareness refers to "the perception of environmental elements in a certain time and space, the specific understanding of their meaning, and the understanding of their situation in the near future. Network security situational awareness, as a type of active defense technology, discovers and analyzes dangerous behaviors in the network, and discovers the risks existing in the network as soon as possible. By sensing the host node, log, topology structure, etc., it can formulate and schedule different security solutions in a timely manner, so that it can reduce losses and reduce risks before the attack arrives.

Situational awareness has emerged as a hot topic in the cyber security industry, due to its capacity to improve decision-making by applying a three-layer model of observation, understanding, and prediction [12, 13]. In the early stage when security situational awareness was proposed, literature [14] proposed a security situational awareness

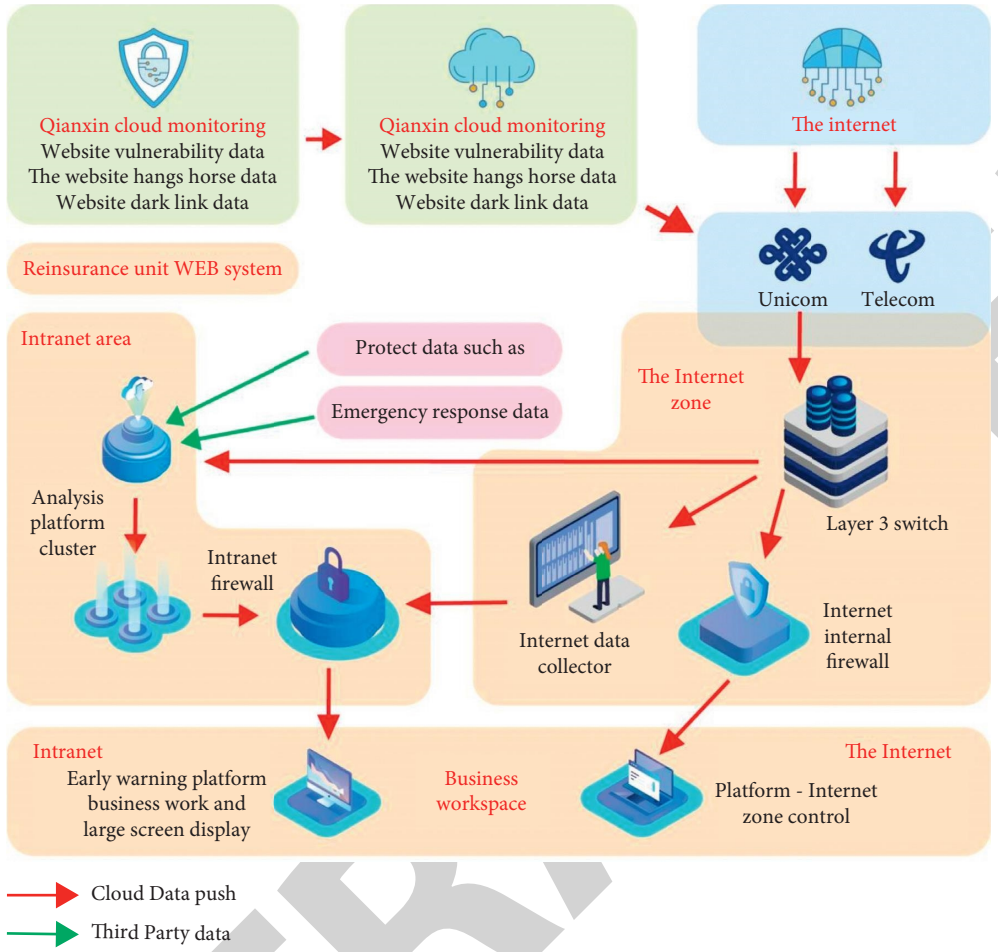

Figure 1: Cyberspace security situational awareness solutions.

model based on simple weighting method and gray theory; literature [14] proposed a network security situational assessment scheme based on attack mode identification; literature [15] summarized the current research direction and found that the research work mainly focused on the simple static evaluation, and the dynamic analysis from the possible transformation of attack activities was seriously insufficient, including early warning analysis and other aspects; Reference [16] discusses that the security situational awareness elements are extracted from the attacker, the defender, and the network environment, and a security situational prediction method based on the analysis of the spatiotemporal dimension is further formed. Reference [17] applies the LAMBDA language to support the elaboration of the template and matching process. In the process of the continuous development of the NSSA system, the literature [18] decomposes an independent attack behavior into multiple different time stages, such as the IKC multi-stage attack model [19], by analyzing the semantics of each attack warning report. Pattern matching is performed on the valid alerts and differentiated attack stages after the configuration information is verified with the vulnerability information to reproduce the complete attack process; reference [20] proposes a network security situation prediction method based on immune time series; reference [21] developed an online visual analysis system OCEANS to deal with network security events to assist users to quickly understand the actual network security situation and reduce the frequency of system false positives; reference [22] also describes a visual analysis system that can ensure security management. Personnel timely discover the actual harm of network security threats to critical infrastructure; reference [23] proposes a situational awareness model that can simultaneously realize information sharing among multiple agencies, which helps to further improve the security situational awareness system and reduce network security hazards caused by risks.

With the deterioration of Internet security, spatial awareness has become a top issue in the area. The breadth and depth of data, business logic with which it is processed, and the clarity and intuitive with which the information is analyzed all influence the effect of situational awareness decision-making processes [24, 25]. Historically, research on network security incidents has made achievements in different fields, but from a macro perspective, they are all scattered. Reference [26] reviewed and summarized the analysis tools of security events in stages, and representative tools include Swatch, SEC, OSSEC, etc. [27] proposed a security event based on data mining. The analysis framework can obtain security events with analytical value from multisource and heterogeneous massive raw data, and further

detect security risks, potential threats, and unknown attacks; Leijiao et al. [28] proposed a graph theory-based method. A trace analysis method is used for understanding the detection and response data of collected incidents, constructing applicable patterns for data classification from attack trajectories. A finite state machine can be constructed based on certain rules to automate data classification, then a state machine can be constructed according to the tracking trajectory, and finally the effectiveness of the state machine and the performance of the state machine can be evaluated; Powar et al. [29] identified specific security events as the starting point to take the development process of the security incident life cycle as the main idea, supplemented by security management and security technology, to build a complete security incident life cycle management and control system.

Security incident emergency response is an important field of security incident research. Hou et al. [30] proposed a set of basic network security incident emergency response linkage schemes, which can reasonably dispatch geographically distributed resources to coordinately respond to the sudden occurrence of network security incidents. According to the characteristics of network security incidents, Reti et al. [31] have pointed out the key point of the network information security incident emergency response (NISIER) system, proposed a new NISIER architecture—"8641" hierarchy, and expounded this system. In order to solve the problem of the combination of network security emergency response system and emergency management platform, Tan et al. [32] proposed a security architecture of a web-based network security emergency management platform, which uses the stored procedure of parameterized statements to further filter hazardous information.

3. Research Methods

In order to provide more comprehensive data for the awareness and understanding stage of network security situational awareness, and to solve the problem that it is difficult for current users to obtain the key information they need in time from hundreds of millions of network security event texts, this paper designs and implements the text processing-based network security event analysis tool. Taking into account the advantages of machine learning algorithms in the fields of text classification and decomposition and information extraction, the actual functions of various tools involved in this chapter are completed by combining them with network security event processing. Figure 2 shows the overall framework of the network security event analysis tool.

3.1. Scrapy Framework Analysis and Application. Scrapy is a robust web crawler framework based on the *Python* language. *Python* has the benefits of being lightweight, simple, and having a wide range of applications, among other characteristics. Several crawler frameworks and application modules based on *Python* are now well developed, with the crawler framework being particularly prominent in the use of generic web crawlers. It can scrape data from various data sources. It is an elevated web crawling and scraping technology for crawling and extracting organized data from online pages. It has a variety of applications, including data mining, surveillance, and automated testing. It can scrape data from various data sources. Scrapy also allows operations such as cleaning, formatting, decorating, and storing these data into data to cascade, so that the performance degradation becomes smaller. Technically, Scrapy is a scraping application built with *Python*'s twisted framework, because Twisted is event-driven, allowing Scrapy to split the throughput through smooth operations when it has thousands of open connections delay. Users can modify it according to their needs, and it is simple and lightweight to use, so it has a wide range of uses and can be used in a series of fields including data mining, information processing, or storage of historical data [33].

When implementing the Scrapy framework, this paper mainly uses the custom crawler module (spider.py), project module (items.py), pipeline module (pipelines.py), and configuration file module (setting.py). When writing the crawler module, according to the characteristics of the actual network security event website, the regular expression of Xpath is used to parse the HTML text from the engine and locate the target information; when writing the project module, the specific crawler is determined Tasks, namely, Title, Category, Summary, Pub-time, Author, and Security Event Content (Article); when writing the pipeline module, according to the website source, the safe time text information is numbered, sorted, and stored separately [34].

3.2. Classification of Network Security Incidents. After referring to China's official classification standards for information security incidents, comprehensively consider that the main research object of this paper is network security incidents, at the same time refer to the triggering rules, nature, and mechanism of network security incidents, and consider the requirements of the current network security situation. Harmful program incidents (MI) and network attack incidents (NAI) in information security incidents are the two main categories of network security incidents, and the specific downward classification of the two categories is shown in Table 1, as the final classification standard of the article [35]. A denial-of-service (DOSAI) attack is a cyber-attack in which the offender attempts to render a computer or network resource inaccessible to its user requirements by temporary or permanently interrupting services of a server attached to the network. A backdoor attack (BDAI) is a sort of hack that exploits security flaws in computer networks. Poor design, code problems, and malware can all generate these vulnerabilities, which might be purposeful or inadvertent. Backdoor attacks are frequently used to obtain unwanted access to networks or data, as well as to infect systems with malware. A botnet assault is a type of cyber-attack that occurs when a collection of World Wide Web devices becomes infected with software controlled by malevolent hackers. Botnet

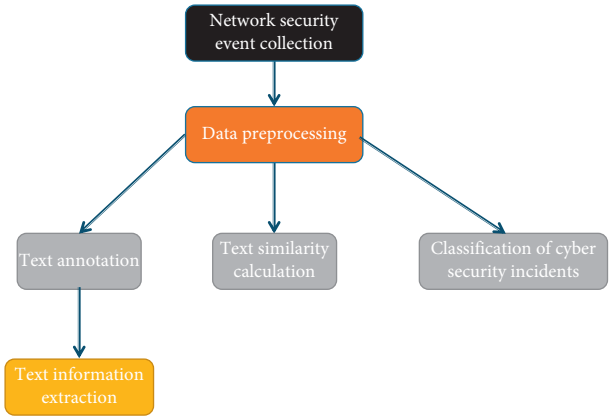

Figure 2: Overall frame diagram.

assaults (BI) often entail spamming, data breaches, stealing confidential material, or conducting devastating DDoS attacks [36].

3.3. Classification Implementation of Crawler Algorithm Based on Neural Network Model. The goal of training a neural network is to input a crawler algorithm training set that has completed text preprocessing and determine the category into the neural network model, so that it can be trained and continuously learned to form rules for recognizing a certain type of text. The implementation process of the classification module is shown in Algorithm 1. First, the determined categories and the eigenvalues extracted by TF-IDF are used as the input of the neural network model, the classification list in the sample set is looped through, and the MLP multilayer perception classification in the sklearn library is used. The processor handles classification problems.

Among the parameters of MLP, solver represents the solver for weight optimization, alpha represents the initial learning rate of the neural network, hidden_layer_sizes represents the number of neurons in the hidden layer, and random_state is the default state or seed without a random number generator [37]. The joblib function saves the training model formed by each loop, and when the traversal of the training samples is completed, the final classification model is formed. Then, by judging whether the actual classification is the same as the model predicted classification, if it is the same as the actual classification, assign a value to the variable representing the accuracy rate, and continuously record the number of correct classifications in the database. If it is different from the actual classification, record it in the database. The number of misclassified cybersecurity events finally returns the overall average classification accuracy.

In this paper, the preprocessed training samples have a total of 9962 feature dimensions, and the network security events are divided into 14 categories. Therefore, the number of neurons in the input layer of the neural network is 9962, the depth of the hidden layer is 1, the number of neurons in the hidden layer is 20, the number of neurons in the output layer is 14, and the learning rate of the model is 2.0.

During supervised learning, the maximum likelihood algorithm is used to calculate the parameter matrix of the model according to the manual annotation results of the training samples, and finally the construction of the information extraction model is completed. The parameters of the HMM model can be calculated by the above crawler algorithm:

$$a_{ij} = \frac{C_{ij}()}{\sum_{k=1}^{n} C_{ik}}, \quad 1 \le i,\ j \le n, \tag{1}$$

where C_{ij} is the frequency of transition from state i to state j and $\sum_{k=1}^{m} C_{ik}$ is the sum of the frequency of transition from state i to all states.

$$b_j(k) = \frac{E_j k()}{\sum_{i=1}^{m} E_j i()}, \quad 1 \le i,\ j \le n \le k \le m, \tag{2}$$

where $E_j k()$ is the frequency at which state j releases observation x_k and $\sum_{i=1}^{m} E_j i()$ is the sum of the frequencies at which state j releases all observations.

4. Analysis of Results

4.1. Test Data Sources. The test source of this paper mainly comes from the VCDB (VERIS Community Database) security event dataset. The network security events obtained by the crawler tool are stored in the MySQL database. The current event database stores a total of 43848 pieces of data, as shown in Table 2. This dataset is designed to collect and disseminate information on cybersecurity incidents for all publicly disclosed data breaches. Its data are encoded in VERIS format, and the same data are published in JSON format in GitHub. Each event in the dataset is a self-contained JSON file, including the original URL used when the data were collected.

4.2. Classification Model Test Experiment. This paper compares the classification accuracy of two text classification algorithms, naive Bayes and logistic regression, and the crawler algorithm based on the neural network model used in this paper. The logistic regression algorithm is a well-known algorithm. The main reason is that it is more efficient, does not require a large amount of calculation, is simple and easy to understand, does not require scaling of input features, hardly requires any special design, is easy to adjust, and can output calibrated predicted probabilities. Another advantage is that it is easier to implement and the model training is more efficient; naive Bayes is one of the most commonly used text classification models, and it has a good effect on datasets with a large degree of discrimination such as information classification. And its model is relatively simple, which can reduce the requirements for the scale of the dataset to a certain extent.

The specific experimental process is to extract 2,000 pieces of data from the three categories of test data, namely, backdoor attack events, vulnerability attack events, and network scanning and eavesdropping events, for a total of 6,000 pieces of data. Starting from 1000 pieces of data,

Table 1: Specific classification of network security incidents.

Unwanted program event (MI)	Cyber-attack incident (NAI)
Computer virus incident (CVI)	Denial-of-service attack (DOSAI)
Worm event (WI)	Backdoor attack (BDAI)
Trojan Horse incident (THI)	Vulnerability attack event (VAI)
Botnet incident (BI)	Network scanning eavesdropping (NSEI)
Hybrid attack program incident (BAI)	Phishing incident (PI)
Web page embedded malicious code event (WBPI)	Disturbance event (II)
Other unwanted program events (OMI)	Other cyber-attack incidents (ONAI)

```
(1)  INPUT: tfidf_path weight and category
(2)  OUTPUT: total_correct_rate
(3)  For each classify_name in classify_list do
(4)      MLPClassifier(hidden_layer_sizes, random_state,
(5)  solver, alpha)
(6)      joblib.dump(network_clf)
(7)      If real_classify = = predicted_classify then
(8)          correct_rate = predicted_score
(9)          correct_file_num = correct_file_num + 1
(10)     Else
(11)         wrong_file_num = wrong_file_num + 1
(12)     End if
(13) Return total_correct_rate
```

Algorithm 1: Crawler algorithm implementation.

Table 2: Examples of VCDB database.

Incident type	Time	Summary
Hacking	May. 2019	Employee accidentally included attachment to e-mail with sensitive information about current/former/deceased students and one teacher
Website defacement	Jan. 2020	Stolen mobile device places PII for over 100,000 people at risk. Device was not encrypted and did not have password protection
Website defacement	N/A. 2019	Hackers part of the anonymous-affiliated k0detec collective have gained unauthorized access to the systems of MOAB training international
Server breach	N/A. 2020	After three long years of investigation by the Federal Bureau of Investigation, a local woman has been indicted in federal court on 26 counts of bank fraud, identity theft, and bankruptcy fraud
Website hacked	May. 2021	External actor conspired with servers to skim customer credit car
Private key stolen	N/A. 2019	Veteran A received veteran B's medication. Information included veteran B's name and medication type

additional 1000 pieces of data are input into three classification models. The experimental results are shown in Figures 3 and 4.

As shown in Figures 3 and 4, it can be seen that the classification accuracy of the neural network is increased by 12.79% and 29.33% compared with logistic regression and naive Bayes, respectively, while the reading time is reduced by 63.5% and 87.2%. The reason is that the keywords of each category in the network security event classification are more uncertain than the news classification. For example, in the news information classification, keywords such as "star,", "drama," and "variety show" generally appear in "entertainment." In category news, keywords such as "athlete," "schedule," and "referee" generally appear in "physical" category news, and keywords of different types have great differences. In the classification of network security incidents, the keyword "attack" has a high probability of occurrence in categories such as "worm incident," "mixed attack program incident," and "backdoor attack incident." It appears frequently in "vulnerability attack events" as well as "interference events," and thus network security event classification frequently requires referring to the connection between numerous keywords at the same time.

Among them, the detection effect of the logistic regression algorithm is the least ideal, because logistic regression belongs to a linear model, the model complexity is relatively low, and the ability to describe the boundary of the sample points with irregular spatial distribution is

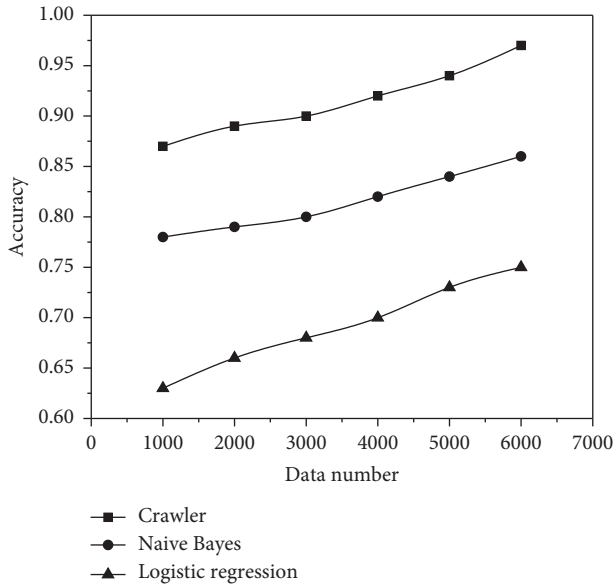

Figure 3: Classification model accuracy comparison.

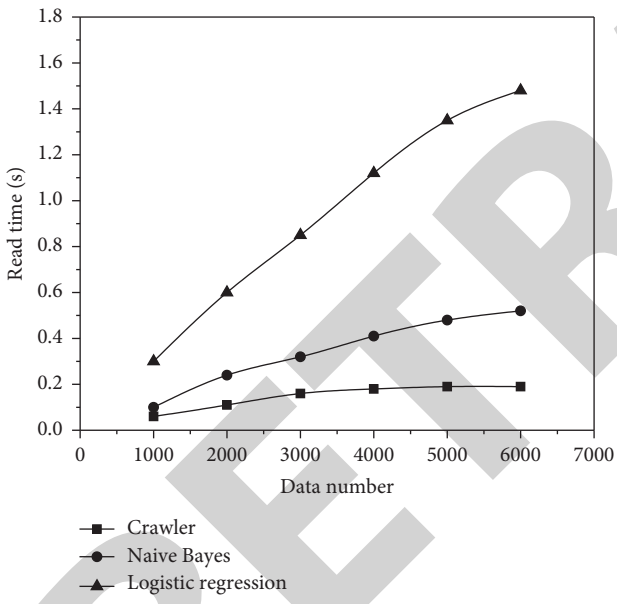

Figure 4: Classification model read time comparison.

insufficient; the prior probability predicts the type of new samples. In order to avoid the formation of exponential parameters when the model is established, it is necessary to assume that each feature (i.e., vocabulary) in the sample is independent of each other. Therefore as a result, when the number of features in the problem is high and each feature has a specific connection between them, this assumption will interfere with the model's prediction effect. From the experimental results, this may limit the further improvement of the accuracy. The neural network algorithm performed the best detection and significantly outperformed the previous algorithm. In contrast, the neural network model simulates the human nervous system by constructing multiple layers of neurons and can gradually extract the intrinsic content between different input neurons (i.e., vocabulary) in the process of optimizing the weights between neurons in each layer. It can express complex nonlinear functional relationships, and the changes in the internal parameters of the algorithm improve the generalization performance, thus achieving superior detection results, so it shows better results in the classification of network security events.

5. Conclusion

The research results of this paper are based on the characteristics of network security events as an important parameter of network security situational awareness research, and combined with machine learning, crawler algorithm, and hyper-network technology, it can quickly distinguish and query the constantly updated network security events, providing users or researchers. It provides great convenience and has strong applicability; at the same time, it can also clearly present the internal connection of network security events. A text processing-based network security event analysis tool is designed and implemented in this study. The real characteristics of the numerous instruments engaged in this article are completed by merging them with network security event processing, taking into consideration the benefits of machine learning algorithms in the domains of text categorization and segmentation and information extraction. Starting from the correlation between security events, it is helpful to establish the impact of security events on network system security. The impact analysis of the degree of impact is also of positive significance for the analysis of real network attacks and defense historical events, as well as the analysis of the development trend of attack and defense technologies; at the same time, the research field of super network has been expanded, and it has been extended to cyberspace security from other fields, which greatly enriched the scope of application of hyper-networks. It can also express complicated nonlinear functional connections, and adjustments to the algorithm's internal parameters increase generalization capability, resulting in superior detection results; thus, it performs better in network security event categorization.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

The authors are thankful to the: 1. The Program of Cultivating Outstanding Young Scientific Research Talents in Universities of Fujian Province: Research on the dissemination and evolution of social network hot events based on game theory and SIRS, ZX17033, Project Leader: Dezhi Wei.

2. The Doctoral Research Initiation Fund Program: Research on robot decision technology based on multi-sensor information fusion, CK18013, Project Leader: Dezhi Wei. 3. Program of Fujian Provincial Department of Education: Modeling and simulation analysis of group behavior in the evolution of social network emergencies, JAT201035, Project Leader: Dezhi Wei. 4. Education and Scientific Research Project for Middle-Aged and Young Teachers in Fujian Province: Research and design of Internet public opinion crawler algorithm based on big data, JT180876, Project Leader: Wu Xu.

References

[1] S. Lu and Y. Zhuang, *A Network Security Situational Awareness Framework Based on Situation Fusion*, 2021.

[2] Y. Zhao, "Application of Machine Learning in Network Security Situational Awareness," in *Proceedings of the 2021 World Conference on Computing and Communication Technologies (WCCCT)*, Dalian, China, January 2021.

[3] G. S. Sriram, "Security challenges of big data computing," *International Research Journal of Modernization in Engineering Technology and Science*, vol. 4, no. 1, pp. 1164–1171, 2022.

[4] H. Li, M. Shabaz, and R. Castillejo-Melgarejo, "Implementation of python data in online translation crawler website design," *International Journal of System Assurance Engineering and Management*, 2021.

[5] D. Bhargava, B. Prasanalakshmi, T. Vaiyapuri, H. Alsulami, S. H. Serbaya, and A. W. Rahmani, "CUCKOO-ANN based novel energy-efficient optimization technique for IoT sensor node modelling," *Wireless Communications and Mobile Computing*, vol. 2022, Article ID 8660245, 9 pages, 2022.

[6] L. Matta and M. Husák, "A Dashboard for Cyber Situational Awareness and Decision Support in Network Security Management," in *Proceedings of the 17th IFIP/IEEE International Symposium on Integrated Network Management (IM 2021)*, IEEE, Bordeaux, France, May 2021.

[7] G. S. Sriram, "Edge computing vs. Cloud computing: an overview of big data challenges and opportunities for large enterprises," *International Research Journal of Modernization in Engineering Technology and Science*, vol. 4, no. 1, pp. 1331–1337, 2022.

[8] S. Zhang, K. Srividya, I. Kakaravada et al., "A Global Optimization Algorithm for Intelligent Electromechanical Control System with Improved Filling Function," *Scientific Programming*, vol. 2022, Article ID 3361027, 10 pages, 2022.

[9] J. Bhola, S. Soni, and G. K. Cheema, "Recent trends for security applications in wireless sensor networks – a technical review," in *Proceedings of the 6th International Conference on Computing for Sustainable Global Development (INDIACom)*, pp. 707–712, New Delhi, India, March 2019.

[10] B. Wang, X. Yao, Y. Jiang, C. Sun, and M. Shabaz, "Design of a real-time monitoring system for smoke and dust in thermal power plants based on improved genetic algorithm," *Journal of Healthcare Engineering*, vol. 2021, Article ID 7212567, 10 pages, 2021.

[11] Y. Zhu and Z. Du, "Research on the key technologies of network security-oriented situation prediction," *Scientific Programming*, vol. 2021, Article ID 5527746, pp. 1–10, 2021.

[12] J. Du, F. Yuan, L. Ding, G. Chen, and X. Liu, "Research on threat information network based on link prediction," *International Journal of Digital Crime and Forensics*, vol. 13, no. 2, pp. 94–102, 2021.

[13] M. Yang, P. Kumar, J. Bhola, and M. Shabaz, "Development of image recognition software based on artificial intelligence algorithm for the efficient sorting of apple fruit," *International Journal of System Assurance Engineering and Management*, vol. 13, 2021.

[14] Y. Zhang, X. Kou, Z. Song, Y. Fan, M. Usman, and V. Jagota, "Research on logistics management layout optimization and real-time application based on nonlinear programming," *Nonlinear Engineering*, vol. 10, no. 1, pp. 526–534, 2021.

[15] W. Qian, H. Lai, Q. Zhu, and K. C. Chang, *Overview of Network Security Situation Awareness Based on Big Data*, 2021.

[16] H. Zhang, C. Kang, and Y. Xiao, "Research on network security situation awareness based on the lstm-dt model," *Sensors*, vol. 21, no. 14, p. 4788, 2021.

[17] N. Kishor, K. Uhlen, L. Vanfretti, and S. Skok, *Synchrophasor Technology: Towards Real-Time Operation of Power Networks*, 2021.

[18] J. Y. Zhang, S. Y. Bi, L. L. Gong, W. W. Kong, and X. Y. Zhang, *Research on Network Optimization and Network Security in Power Wireless Private Network*, 2021.

[19] W. Li and H. Zhu, "Research on Comprehensive Enterprise Network Security," in *Proceedings of the 2021 IEEE 11th International Conference on Electronics Information and Emergency Communication (ICEIEC)*, IEEE, China, June 2021.

[20] X. He, "Research on computer network security based on firewall technology," *Journal of Physics: Conference Series*, vol. 1744, no. 4, Article ID 042037, 2021.

[21] Z. Zou, T. Chen, J. Chen, Y. Hou, and R. Yang, "Research on Network Security Risk and Security Countermeasures of 5G Technology in Power System Application," in *Proceedings of the 2021 IEEE 5th advanced information technology, electronic and automation control conference (IAEAC)*, Beijing China, October 2021.

[22] T. K. Lohani, M. T. Ayana, A. K. Mohammed, M. Shabaz, G. Dhiman, and V. Jagota, "A comprehensive approach of hydrological issues related to ground water using GIS in the Hindu holy city of Gaya, India," *World Journal of Engineering*, p. 6, 2021.

[23] N. Ding, P. Prabhakar, A. Khosla, V. Jagota, E. Ramirez-Asis, and B. K. Singh, "Application of fuzzy immune algorithm and soft computing in the design of 2-DOF PID controller," *Discrete Dynamics in Nature and Society*, vol. 2022, Article ID 5608054, 8 pages, 2022.

[24] Z. Yan, Y. Yu, and M. Shabaz, "Optimization research on deep learning and temporal segmentation algorithm of video shot in basketball games," *Computational Intelligence and Neuroscience*, vol. 2021, pp. 1–10, 2021.

[25] G. S. Sriram, "Green cloud computing: an approach towards sustainability," *International Research Journal of Modernization in Engineering Technology and Science*, vol. 4, no. 1, pp. 1263–1268, 2022.

[26] J. Zhao, "Research on network security defence based on big data clustering algorithms," *International Journal of Information and Computer Security*, vol. 15, no. 4, p. 343, 2021.

[27] H. Song, D. Zhao, and C. Yuan, "Network security situation prediction of improved lanchester equation based on time action factor," *Mobile Networks and Applications*, vol. 26, no. 3, pp. 1008–1023, 2021.

[28] L. GeGe, Y. LiLi, S. LiLi, J. Zhu, and J. Yan, "Evaluation of the situational awareness effects for smart distribution networks under the novel design of indicator framework and hybrid

weighting method," *Frontiers in Energy*, vol. 15, no. 1, pp. 143–158, 2021.

[29] V. Powar and R. Singh, "Stand-alone direct current power network based on photovoltaics and lithium-ion batteries for reverse osmosis desalination plant," *Energies*, vol. 14, no. 10, p. 2772, 2021.

[30] R. Hou, G. Ren, W. Gao, and L. Liu, "Research on cyberspace multi-objective security algorithm and decision mechanism of energy internet," *Future Generation Computer Systems*, vol. 120, no. 10, pp. 119–124, 2021.

[31] D. Reti, D. Klaasen, S. D. Anton, and H. D. Schotten, "Secure (S) Hell: Introducing an SSH Deception Proxy Framework," in *Proceedings of the 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, Dublin, Ireland, June 2021.

[32] L. Tan, K. Yu, F. Ming, X. Chen, and G. Srivastava, *IEEE Consumer Electronics Magazine*, no. 99, p. 1, 2021.

[33] H. Liu, "Quantitative situational awareness algorithm of land state network based on neutral statistics," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–11, 2021.

[34] J. Pyhnen, J. Rajamki, V. Nuojua, and M. Lehto, *Cyber Situational Awareness in Critical Infrastructure Organizations*, 2021.

[35] J. Chen, T. Yang, B. He, and L. He, *An Analysis and Research on Wireless Network Security Dataset. 2021 International Conference on Big Data Analysis and Computer Science (BDACS)*, 2021.

[36] J. Bhola and S. Soni, "Information theory-based defense mechanism against DDOS attacks for WSAN. Advances in VLSI, communication, and signal processing," *Lecture Notes in Electrical Engineering*, vol. 683, 2021.

[37] B. Yang, Y. Yu, Z. Wang et al., "Research on network security protection of application-oriented supercomputing center based on multi-level defense and moderate principle," *Journal of Physics: Conference Series*, vol. 1828, no. 1, Article ID 012114, 2021.