International Journal for Housing Science and Its Applications
Publish August 4, 2025. Volume 46, Issue 3 Pages 2729-2739

https://doi.org/10.70517/ijhsa463230

Construction and Optimization of a Decision-Making Model for Cybersecurity Expert Systems Based on Multi-Source Data

He Li[1,*]
[1] School of Cyber Science and Engineering, Southeast University, Nanjing, Jiangsu, 211189, China
Corresponding authors: (e-mail: lhzjxtei@126.com).

Abstract Aiming at the problem that it is difficult to accurately detect network malicious activities and unable to effectively analyze the network condition with single-point network data, this paper introduces the improved DS evidence theory, constructs a network security multi-source heterogeneous data fusion model, and applies the model to assess the network security posture on the basis of ensuring the model's effectiveness and finally realizes the design of network security expert system. The experimental results show that compared with the recognition technology based on PSO-TSA model and the recognition method of network security posture elements based on clustering algorithm, the DS recognition framework in the data fusion model of this paper is able to recognize the network information security posture elements more accurately, and it can effectively safeguard the network information security to adapt to the increasingly complex network environment. Network security expert system managers should pay attention to assessing the network security posture from the service, host, network and other levels, and take targeted measures. The system in this paper is able to understand complex network security issues and provide targeted solutions and recommendations, which can greatly improve the response speed and processing quality of network security incidents.

Index Terms DS evidence theory, multi-source heterogeneous data, data fusion, network security, expert system

I. Introduction

With the rapid development of information technology and the increasing prominence of cybersecurity issues, the role of cybersecurity expert systems has become increasingly important [1], [2]. A network security expert system is a software system that provides intelligent decision support for diverse and complex network security problems by modeling the knowledge and experience of network security experts [3], [4]. The goal of network security expert system is to ensure the security and reliability of the network system, to protect the privacy and data security of users, to prevent network attacks and illegal invasion, to improve the anti-attack ability and recovery ability of the network system, and to safeguard the normal operation of the network system and the continuous development of the business [5]-[8].

One of the important responsibilities of the network security expert system is to identify and resolve network security vulnerabilities, and the system needs to discover potential vulnerabilities and weaknesses by conducting a comprehensive security assessment of the network system [9], [10]. This includes auditing network devices, operating systems, applications, and databases to ensure that they are resistant to various attacks [11], [12]. Cybersecurity expert systems also need to fix the discovered vulnerabilities in a timely manner and develop appropriate security measures to prevent future attacks [13], [14]. Second, the network security expert system needs to develop a comprehensive security policy based on the requirements and risk assessment [15]. This includes the development of password policy, access control policy, data backup policy, etc [16]. Only by establishing a perfect network security expert system and adopting effective security measures and security strategies can we effectively deal with all kinds of network security threats and risk issues, and protect the security of network systems, so in the application of network security expert system, the decisions it makes need to be optimized [17]-[20].

This paper proposes a data fusion framework based on the improved DS evidence theory and realizes the construction of a cybersecurity multi-source heterogeneous data fusion model based on it, which mainly contains a data preprocessing module, a DS recognition framework, a BPA confidence function assignment module and an evidence decision module. In order to assess the effectiveness of the model, the model is used to conduct network security posture assessment experiments. Finally, a network security expert system based on multi-source heterogeneous data fusion is designed with the model of this paper as the core.

II. Cybersecurity data fusion model based on DS evidence theory

This chapter constructs a fusion model of multi-source heterogeneous data for cybersecurity based on the improved DS evidence theory to provide modeling tools for the design of cybersecurity expert systems.

II. A.Improved DS Theory of Evidence Convergence Framework

The Dempster's combination rule in the classical D-S theory of evidence [21] is flawed in that the larger its conflict coefficient k, the greater the conflict. When $k=1$, the conflict between the evidence is serious, and the combination rule fails. In order to overcome the shortcoming, many scholars have proposed different improvement methods, which can be categorized into methods based on modifying Dempster's combination rule and methods based on modifying the original source of evidence according to their principles.

In this paper, we propose a conflict evidence synthesis rule based on the similarity coefficient between the evidence, and give the calculation method of the new weights, which is as follows.

Let m_1 and m_2 be the basic trust assignments of evidences E_1 and E_2, and p_i and q_j be the corresponding joule elements of the two evidences, respectively, and the similarity coefficients α between the two evidences are:

$$\alpha_{12}=\frac{\sum_{p_i\cap q_j\neq\phi} m_1(p_i)m_2(q_j)}{\sqrt{(\sum m_1^2(p_i))(\sum m_2^2(q_j))}} \tag{1}$$

From equation (1), we can see that $\alpha_{12}=\alpha_{21}$. This coefficient is used to describe the similarity between two evidences, and its value ranges from 0 to 1. The larger the value means the smaller the conflict between evidences, and vice versa, the larger the conflict.

For the case of n groups of evidence, the similarity coefficient matrix of the evidence can be obtained according to equation (1):

$$A=\begin{bmatrix} 1 & \alpha_{12} & \cdots & \alpha_{1n} \\ \alpha_{21} & 1 & \cdots & \alpha_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ \alpha_{n1} & \alpha_{n2} & \cdots & 1 \end{bmatrix}_{n\times n} \tag{2}$$

The sum of the elements in each row of the matrix A represents the support for the evidence E_i, i.e:

$$Z(m^i)=\sum_{j=1}^{n}\alpha_{ij} \quad i,j=1,2,\cdots,n \tag{3}$$

Normalizing them gives the credibility of the evidence E_i as:

$$K(m_i)=\frac{Z(m_i)}{\sum_{i=1}^{n}Z(m_i)} \quad i=1,2,\cdots,n \tag{4}$$

The larger credibility $K(m_i)$ indicates that the evidence E_i is more credible, and vice versa. In this paper, we use the credibility to represent the weight of the evidence, and use this weight to weight and average the basic trust allocation of the original evidence to get a new basic probability allocation function, and then perform $n-1$ times synthesis.

According to the improved weighted evidence theory algorithm [22], this paper proposes an improved D-S evidence theory fusion framework. First, the monitoring data are preprocessed, and then the damage features are calculated according to different damage feature index calculation methods, and these damage features are normalized as BPA.Then, the conflict coefficient between the evidences is calculated, and if the value of the conflict coefficient is less than 0.9, the evidence fusion is performed by using the ordinary Dempster combination rule. If the conflict coefficient is greater than or equal to 0.9, the improved conflict evidence fusion method is used for fusion. Finally, the results of each evidence fusion are output.

II. B.Network security multi-source heterogeneous data fusion model construction

The goal of the model in this paper is to realize data fusion of traffic data monitored by multi-network sensors and alarm data given. Considering that the goal of the model in this paper is to minimize redundant data without losing the meaning of the data in order to provide a data-level foundation for security situational awareness, the model should mainly contain a data preprocessing module, a DS recognition framework, a BPA confidence function assignment module, and an evidence decision module.

The multi-source heterogeneous data fusion process is shown in Fig. 1.

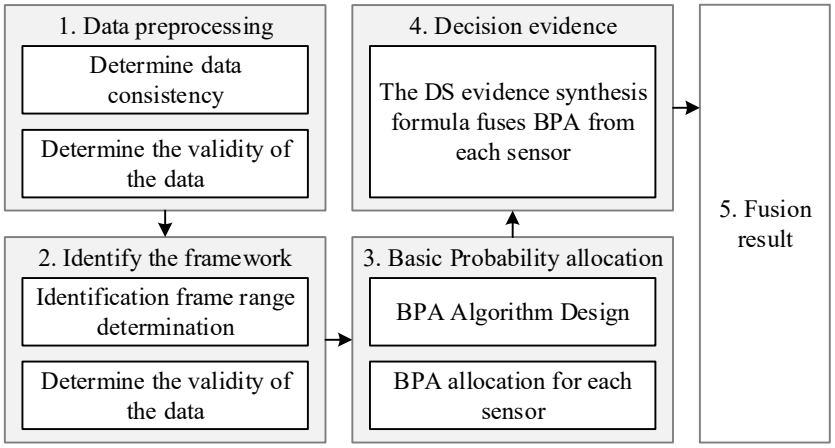


Figure 1: Multi-source heterogeneous data fusion process

II. B. 1) Data pre-processing sessions

In the data preprocessing stage, the required attributes should be selected, and the useless attribute information should be removed, and only the information related to network attacks should be retained. Different data sources, such as system logs, traffic sensors at different levels, and firewalls, should be filtered according to different needs, and a corresponding rule base should be established.

II. B. 2) Defining the basic identification framework

The main concern in the cybersecurity posture in the field of market regulation is the accuracy of the type of attack, the identification framework of this paper Θ that is, for multi-sensors as well as security software and so on can detect all the attacks, in the actual dataset, according to the different points of concern, for the traffic sensor mainly contains two types of attack utilization and malware attacks. In the attack utilization mainly contains weak password, misconfiguration, information leakage and other attacks to take advantage of the four kinds of attacks. In the malware mainly contains remote control Trojan horse and rogue promotion two kinds of attacks, for some packet capture analysis tools such as PCAP logs mainly contain specific attacks such as port scanning, SYN flooding, denial of service, XSS cross-site scripting attacks. For different information formats, consider the establishment of the corresponding identification framework respectively, that is, for the traffic sensor for all possible results:

$$R = \{'' r_1 : weak\ password'' ,'' r_2 : Improper\ configuration'' ,'''' ,...'''' , \\ '' r_n : malware''\} \tag{5}$$

And for PCAP, it may turn out to be just that:

$$R = \{'' r_1 : PortScan'' ,'' r_2 : SYNflood'' ,'' r_3 : Dos'' ,'' r_4 : WebAttack'' , \\ '' r_5 : Infilterration''\} \tag{6}$$

Its recognition framework is:

$$\Theta = \{\{\phi\},\{r_1\},\{r_2\},\cdots,\{r_4 r_5\},\cdots,\{R\}\} \tag{7}$$

Both are completely different and give different results. Based on the data sources of market regulation, partial identification frameworks corresponding to different information are obtained as shown in Table 1. After determining the identification framework, basic probability assignments need to be made for each category.

Table 1: Partial Source Identification Framework

Data source	Flow sensor	Host Log	Firewall log
r_1	Weak password	Error event	Port scanning
r_2	APT event	User overstepping authority	SYN flood
r_3	XSS attack	Review event	DoS
r_4	Code execution	Illegal access	SQL injection
r_5	Remote control Trojan	Illegal enforcement	Intrusion alert

II. B. 3) Basic Probability Distribution Functions

Because of the complexity of cybersecurity data in the field of market regulation and the existence of possible false alarms, the basic probability allocation cannot be directly based on the statistical and then normalized method, but a dynamic method should be used for the basic credibility allocation. In this paper, a dynamic recursive formula is established for the basic credibility allocation:

$$J_r = \left(1 - \frac{N_i}{\sum_{i=1}^{n} N_i + N_0}\right) J_{T-1} + \frac{N_i(1-U_{T-1})}{\sum_{i=1}^{n} N_i + N_0} \tag{8}$$

where J_T denotes the level of trust in judging such alerts in the T th cycle, and J_{T-1} denotes the level of trust in such alerts computed by this sensor in the previous cycle. $\sum_{i}^{n} N_i$ is the total number of such alerts acquired by all sensors in the T th cycle. U_{T-1} denotes the ratio of correct and incorrect alarm judgments obtained in the previous cycle's judgments, $U_{T-1}=0$ means that the alarms are correct >50%, and $U_{T-1}=1$ means that the false alarms are >50%, which is determined by the comparison of the fusion results of the previous cycle with the actual situation. N_i denotes the total number of such alerts acquired by the i th sensor in the T th cycle. N_o is a constant to control the convergence rate. The basic BPA probability assignments for the partial alerts in the T th cycle for the partial recognition framework of the flow sensors are obtained after computation.

Data fusion is performed by applying the Dempster fusion rule, and data from multiple data sources with the same recognition frame are synthesized by applying Eq. (9) to them:

$$(m_1 \oplus m_2 \oplus \cdots \oplus m_n)(A) = \frac{1}{K} \sum_{A_1 \cap A_2 \cap \ldots \cap A_n} m_1(A_1) \cdot m_2(A_2) \ldots m_n(A_n) \tag{9}$$

Since propositions in the identification framework are mutually exclusive, both the confidence function and the likelihood function are equal to the synthesized confidence function assignment. Thus the synthesized confidence values can be directly utilized for network security situation analysis.

II. B. 4) Similarity analysis

Due to the different dimensions of the attacker's attack, the attacker may simultaneously carry out multi-directional attacks on the market regulatory system, and the identification framework between different data sources is not conflicting, so the analysis of the network security situation obtained from data sources with different identification frameworks needs to be analyzed in terms of the similarity analysis of the attack.

(1) Attack source address and target address similarity calculation

There are two IP addresses A and B, if any:

$$IP_A \,\&\, Mask_A = IP_B \,\&\, Mask_B \tag{10}$$

Then it is determined that A and B belong to the same network segment, i.e., they have similarity, where Mask denotes subnet mask and “&” denotes with operation.

(2) Time similarity judgment

Since time has continuity, the similarity of time attributes can be directly measured using Euclidean distance. Suppose the time vectors of two alerts are $a=(a_y,a_m,a_d,a_h,a_{ms})$ and $b=(b_y,b_m,b_d,b_h,b_m,b_{ms}s)$, then the temporal similarity of the two alerts can be defined as:

$$d(a,b)=\sqrt{w_y(a_y-b_y)^2+w_m(a_m-b_m)^2+\cdots+w_s(a_s-b_s)^2} \tag{11}$$

where $w_i, i\in(y,m,d,h,m,s)$ is the corresponding weight value of each item.

After determining the similarity of each attribute the combined similarity needs to be judged. Namely:

$$S(a,b)=\sum_{k=1}^{n}W^k S_{ij}^k \tag{12}$$

III. Model application experiments and analysis of results

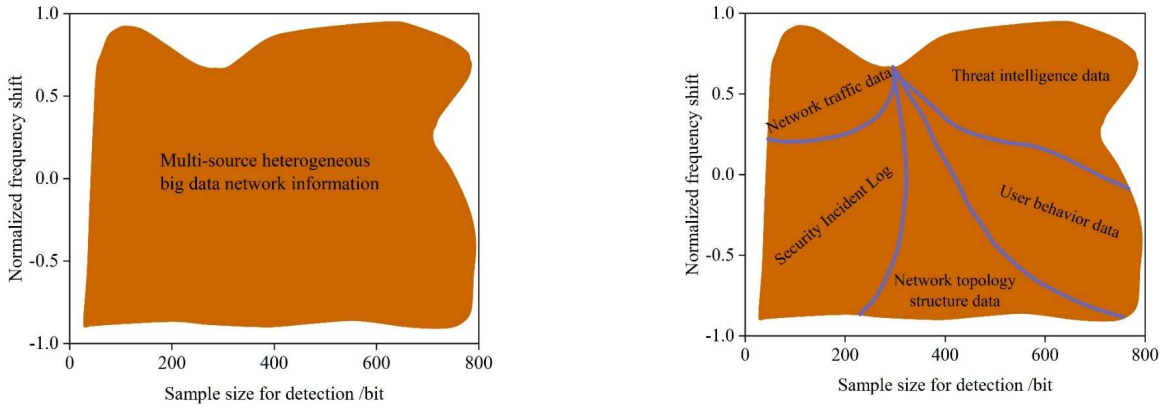
This chapter conducts application experiments on the proposed cybersecurity data fusion model based on the improved DS evidence theory to explore the effectiveness of the DS identification framework in the model in cybersecurity posture identification, evaluate the performance of the model for data fusion, and apply the model for cybersecurity posture instance evaluation.

III. A. Model performance evaluation experiments

III. A. 1) Experimental setup

The information security posture element recognition spectrum of multi-source heterogeneous big data network is used as an experimental parameter to recognize the security posture elements by analyzing the network signal spectrum. The display results of the security posture element identification spectrum at different times are shown in Fig. 2, (a) and (b) represent the security posture element identification spectrum when the time is 1ms and 10ms, respectively.

From the figure, it can be seen that when the time is 1ms, the normalized frequency shift distribution is holistic. When the time is 10ms, the normalized frequency shift distribution is more obvious, and the actual security posture elements thus obtained are threat intelligence data, network traffic data, security event logs, user behavior data, and network topology data.



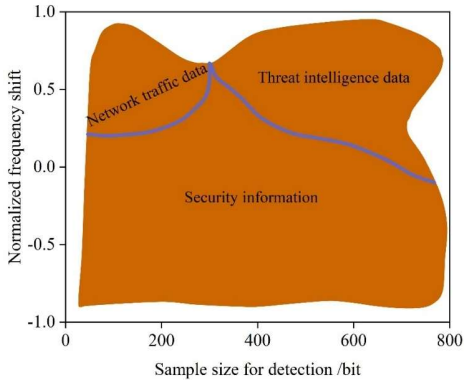
(a) 1ms (b) 10ms

Figure 2: Spectrum of security situation element identification at different times

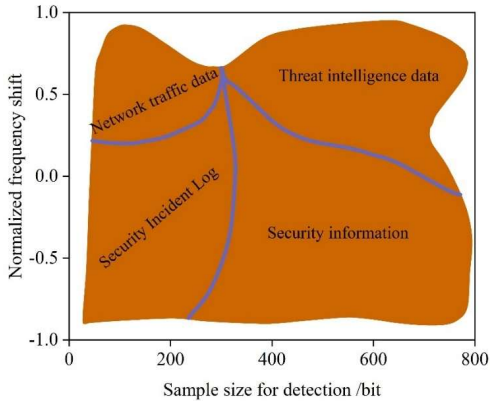
III. A. 2) Experimental results and analysis

The identification technology based on the PSO-TSA model and the network security situation element identification method based on the clustering algorithm are used as the comparison methods of the DS recognition framework in the data fusion model in this paper, and the comparison results are shown in Figure 3, and (a)~(c) represent the security situation element identification spectrum based on the PSO-TSA model, the clustering algorithm and the DS recognition framework in this paper, respectively.

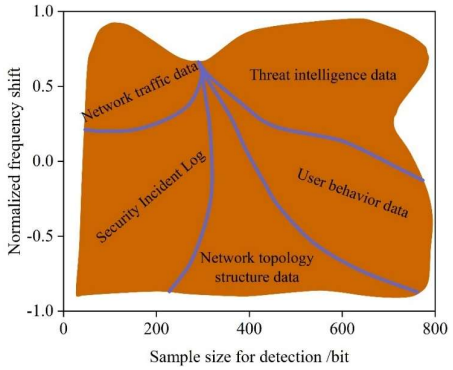
It can be seen that the DS identification framework using the multi-source heterogeneous data fusion model of this paper can accurately identify threat intelligence data, network traffic data, security event logs, user behavior data, and network topology data, and the similarity with the identification results in Fig. 2(b) is high, which indicates that the identification results of this paper's method are more accurate.



(a) PSO-TSA model



(b) Clustering algorithm



(c) The model of this article

Figure 3: Comparative analysis of spectrum identification results by different methods

In order to further verify the accuracy of the recognition results of different methods, the recognition error is used as an experimental index, and the formula is:

$$e = 1 - \frac{N_T + N_P}{N_T + N_P + M_T + M_P} \tag{13}$$

where N_T, N_p denote the number of samples whose samples are correctly recognized and the number of attack samples, respectively, and M_T, M_p denote the number of samples whose attack samples and normal samples are incorrectly identified, respectively. The smaller the calculated result of Eq. (13) is, the more accurate the recognition result is. The resulting recognition error results for different methods are shown in Table 2.

As can be seen from Table 2, the recognition error using the studied method is lower compared to the other two methods, especially for the dataset of security event logs, user behavior data, and network topology data recognition results reflect more obvious.

Table 2: Comparative Analysis of Recognition Errors by Different Methods

Experimental set	Identification error		
	PSO-TSA model	Clustering algorithm	The method of this article
Threat intelligence data	0.25	0.18	0.06
Network traffic data	0.12	0.10	0.09
Security Incident log	0.57	0.28	0.06
User behavior data	0.69	0.55	0.06
Network topology structure data	0.78	0.52	0.09

III. B. Cybersecurity posture assessment

III. B. 1) Service layer posture

Part of the traffic data of 2024-3-26 in UNSW-NB15 is replayed in the network, which lasts for 36000s, and every 5min is a time window, with a total of 120 time windows, e.g., the horizontal coordinate 20 corresponds to the posture value of the 20th time window. Using the network attack threat division principle and weight factor theory proposed in this paper to get the attack factor, according to the evaluation system. The posture of the three services, DNS, HTTP and SMTP, on a particular host is shown in Figure 4.

The HTTP service on this host suffered 3 strong attacks, 5 moderate attacks, and many light attacks on that day. Administrators should pay attention to the use of the HTTP service on this host, whether the host is accessing illegal websites, and whether it is subject to web attacks, and take countermeasures accordingly.

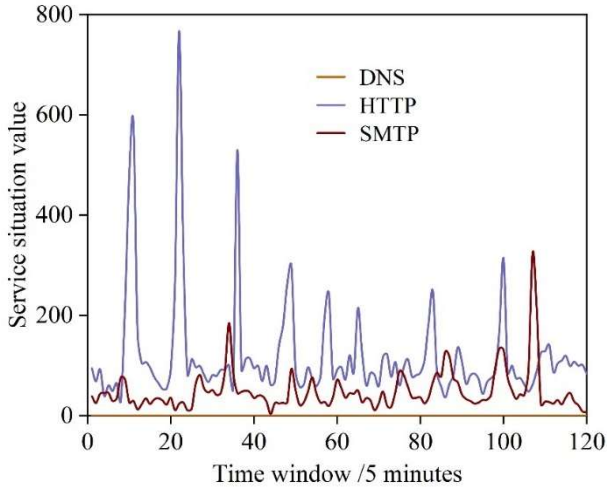


Figure 4: Security situation of the service layer

III. B. 2) Host Layer Posture

The host layer posture is related to the service posture and the importance of each service running on the host, and the weight of the service is determined based on the number of users and frequency of use of the service. The host layer security posture is shown in Figure 5. It can be seen that host 1 was subjected to 2 strong attacks and several medium and small attacks. Host 2 was subjected to 3 strong attacks and host 3 was subjected to 6 strong network attacks. Network administrators should pay special attention to the operation of these two hosts.

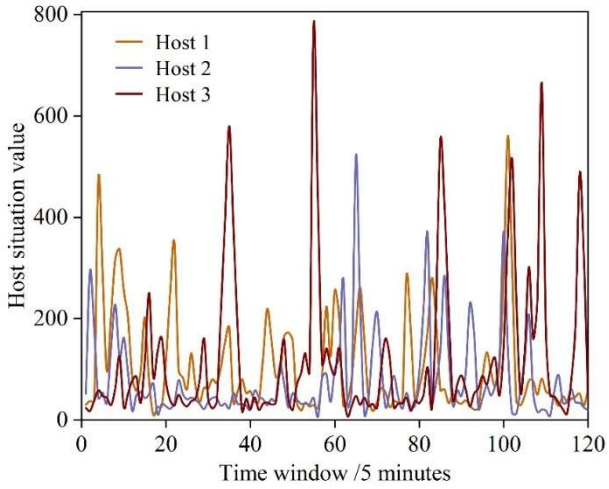


Figure 5: Security situation of host

III. B. 3) Network layer posture

Based on the number of users and frequency of the hosts, the weights of the hosts are determined. Based on the host's weights and the host's posture situation, the operational posture of the entire network is calculated. The

network layer security posture situation is shown in Figure 6, which shows that this network has been continuously attacked in one day, generating five large fluctuations, and the network administrator should check the operation of the hosts in these time periods to find the abnormal hosts. This traffic packet has been subjected to a large number of attacks throughout the day, and the network posture diagram conforms to the traffic packet attacks and accurately shows the operation of the network on that day.

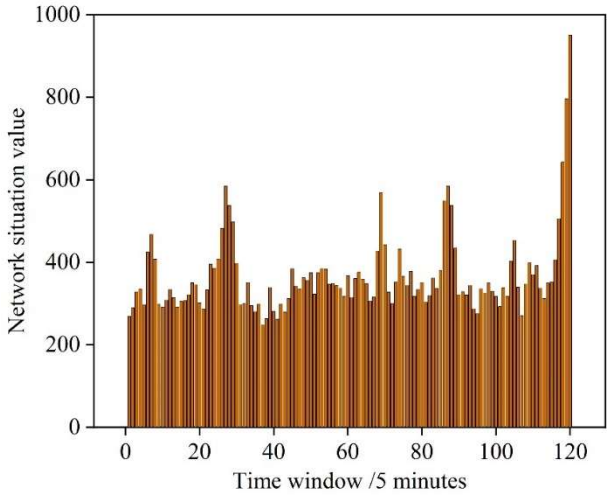


Figure 6: Security situation of network

IV. Design of a network security expert system based on the fusion of heterogeneous data from multiple sources

Based on the improved DS evidence theory to realize the fusion of multi-source heterogeneous data for cybersecurity, this paper designs a cybersecurity expert system, which employs ChatGLM-6B and Langchain technology, in order to provide a new solution for cybersecurity analysis.

IV. A. Overall system framework design

The overall architecture of this expert system is designed as shown in Figure 7, which mainly contains four modules such as knowledge base construction module, similarity indexing module, large model application module user interface module.

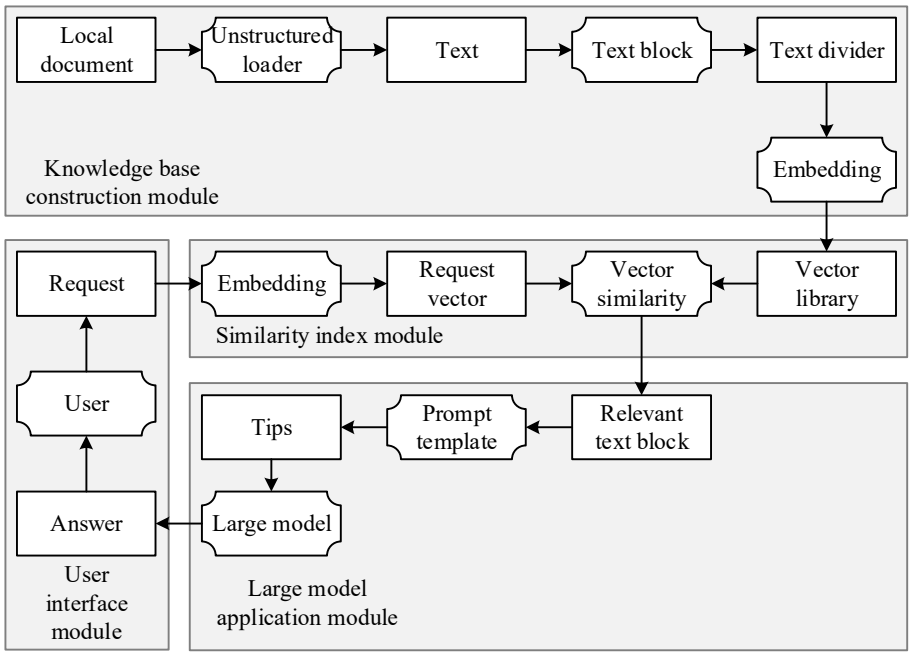


Figure 7: Overall Architecture design of the expert system

IV. B. System module implementation

IV. B. 1) Knowledge base building module implementation

In the network security expert system, the knowledge base module stores a large amount of historical security data, which can support complex decision-making and provide rapid response capabilities to help the system effectively identify and respond to security threats. Its construction process is as follows:

(1) Data collection

In the data collection phase, the main collection of security knowledge documents within the enterprise and the threat intelligence of the security operation and maintenance center in the past 6 months, and supplemented with some information on vulnerabilities and patching strategies from the open data source CVE.

(2) Data Processing

The collected heterogeneous data from multiple sources need to be structured, firstly, the text data is parsed from the file content by UnstructuredFileLoader and cleaned, and then the processed text is encapsulated into a Document object, attaching the necessary metadata information, and further segmenting the long text data to ensure that the final output of text block length is appropriate.

(3) Data vectorization

In this paper, text2vecbase-chinese-paraphrase is chosen as the vector embedding model to transform the processed input text content into vectors. The model is generated based on CoSENT technology and ERNIE 3.0 Base pre-training model, which accurately captures inter-word relations through the attention mechanism and calculates the semantic similarity between sentences with a fixed-dimension vector representation of semantics combined with cosine similarity. Finally, it shows high query processing ability and accuracy on multiple Natural Language Inference (NLI) test set intervals.

(4) Vector Data Storage

In order to efficiently process and retrieve vector data, this paper chooses to use the Milvus database, which supports both horizontal and vertical scaling to accommodate growing data and query requirements, as well as multiple index construction strategies, and the rich parameters provided allow for optimization based on specific query efficiency and accuracy requirements. Finally, the constructed knowledge base is externalized to the Langchain framework through a data interface and synchronization mechanism, and the knowledge base is regularly synchronized and updated, which enhances the system's ability to respond to emerging threats.

IV. B. 2) Similarity Indexing Module Implementation

In this paper, the cosine similarity metric was chosen for the similarity indexing module [23]. In contrast, several other similarity metrics have their own limitations. The workflow of the similarity indexing module is shown in Fig. 8, when a user sends a text Query, it will be transformed into a vector by the Embedding model and the similarity will be calculated with the knowledge in the vector library, vector relevance retrieval will be performed, and after retrieving the Top K knowledge that has the highest relevance to the Query, the text block of the corresponding knowledge will be obtained.

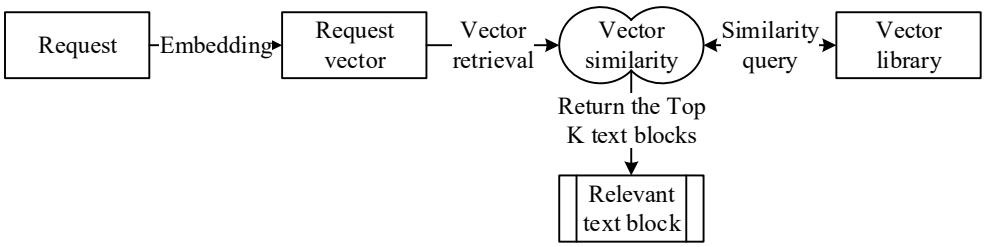


Figure 8: Similarity retrieval process

IV. B. 3) Large Model Application Module Implementation

ChatGLM-6B is a language model with 6.2 billion parameters, which is trained on 1T amount of tokens on 1:1 ratio of Chinese and English materials, both of which are bilingual, which makes the model more suitable for processing Chinese tasks than other open source models. Secondly, drawing on the experience of GLM-130BP training, the two-dimensional RotaryPositional Embedding (ROPE) positional encoding implementation is modified to use the traditional Feedforward Network (FFN) structure. And combined with the model quantization technique, it requires only 13GB of video memory for inference at FP16 accuracy, which enables users to deploy locally on consumer-grade graphics cards, which is not available in other open-source large models. At runtime the module will take the knowledge blocks obtained from the above indexing module and fill them into the user-specified prompt template

to form a complete prompt, which is eventually sent to the big model, which makes an answer based on the prompt, and the application sends the answer to the user interface to present it to the user.

IV. B. 4) User interface module implementation

Gradio is an open source Python library that provides a concise API that allows researchers to quickly generate visual interfaces for models for the Web, and this ease of use greatly lowers the technical barrier. Secondly Gradio supports a variety of input and output forms such as text, images, and audio, and its ability to handle multimedia content and complex interactions exceeds that of tools such as Dash. In addition Gradio provides integration with mainstream frameworks such as TensorFlow, PyTorch, Hugging Face Transformers, etc., which further simplifies the deployment process of the model.

The user interface page contains mainly a text input box to accept user input and a numeric input box for the number of historical dialog arguments to record the number of dialog rounds. It also contains four drop-down selection boxes, Current Session for selecting a different session history, Dialogue Mode for selecting whether to use the LLM dialogue directly or to conduct a dialogue with the LLM based on the knowledge base, selecting the LLM model, and Prompt Template for selecting a predefined Prompt to process the Query content. Slider Temperature is used to express the dispersion of the model's answers, proportional to the size. Finally, two buttons, Export Record and Empty Conversation, were added for processing historical conversation data.

V. Conclusion

This paper introduces the improved DS evidence theory, constructs a multi-source heterogeneous data fusion model for network security, and realizes the design of network security expert system for multi-source heterogeneous data fusion on this basis.

Using the DS identification framework of the multi-source heterogeneous data fusion model in this paper, threat intelligence data, network traffic data, security event logs, user behavior data, and network topology data can be accurately identified. Comparing the network security posture element identification methods based on PSO-TSA model and clustering algorithm, the similarity between this paper's method and the spectrum of security posture element identification when the time is 10ms is higher, indicating that the identification results of this paper's method are more accurate.

The results of the network security posture assessment show that the HTTP service on the host has suffered three strong attacks, five moderate attacks, and many light attacks, and administrators should pay attention to the use of the HTTP service on the host, whether the host is accessing an illegal website, and whether it is subject to a web attack, and take countermeasures accordingly. Meanwhile, the network is continuously attacked in one day, generating five large fluctuations, and the network administrator should check the operation of the hosts in these time periods to find the abnormal hosts. Among them, host 2 and host 3 were strongly attacked 3 times and 6 times respectively, and network administrators should pay special attention to their operation.

Finally, this paper constructs a network security expert system that mainly contains four modules, including knowledge base construction module, similarity indexing module, large model application module user interface module, etc., which provides a new analysis solution for network security.

References

[1] Chivukula, R., Lakshmi, T. J., Kandula, L. R. R., & Alla, K. (2021, November). A study of cyber security issues and challenges. In 2021 IEEE Bombay Section Signature Conference (IBSSC) (pp. 1-5). IEEE.

[2] Li, Y., & Li, X. (2021). Research on Multi-Target Network Security Assessment with Attack Graph Expert System Model. Scientific Programming, 2021(1), 9921731.

[3] Piech, H., & Grodzki, G. (2017). Audit expert system of communication security assessment. Procedia computer science, 112, 147-156.

[4] Mahdavifar, S., & Ghorbani, A. A. (2020). DeNNeS: deep embedded neural network expert system for detecting cyber attacks. Neural Computing and Applications, 32(18), 14753-14780.

[5] Zolkin, A. L., Losev, A. N., Gridina, D. V., & Aygumov, T. G. (2021, February). Research of problems of computer networks expert systems. In IOP Conference Series: Materials Science and Engineering (Vol. 1047, No. 1, p. 012106). IOP Publishing.

[6] Abdymanapov, S. A., Muratbekov, M., Altynbek, S., & Barlybayev, A. (2021). Fuzzy expert system of information security risk assessment on the example of analysis learning management systems. IEEE Access, 9, 156556-156565

[7] Tan, C. F., Wahidin, L. S., Khalil, S. N., Tamaldin, N., Hu, J., & Rauterberg, G. W. M. (2016). The application of expert system: A review of research and applications. ARPN Journal of Engineering and Applied Sciences, 11(4), 2448-2453.

[8] Zhou, Z. J., Hu, G. Y., Hu, C. H., Wen, C. L., & Chang, L. L. (2019). A survey of belief rule-base expert system. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 51(8), 4944-4958.

[9] Sosnovich, A., Grumberg, O., & Nakibly, G. (2013, July). Finding security vulnerabilities in a network protocol using parameterized systems. In International Conference on Computer Aided Verification (pp. 724-739). Berlin, Heidelberg: Springer Berlin Heidelberg.

[10] Pradhan, A., & Mathew, R. (2020). Solutions to vulnerabilities and threats in software defined networking (SDN). Procedia Computer Science, 171, 2581-2589.

[11] Temizkan, O., Park, S., & Saydam, C. (2017). Software diversity for improved network security: Optimal distribution of software-based shared vulnerabilities. Information Systems Research, 28(4), 828-849.
[12] Izhar, M. O. H. D., & Singh, V. R. (2014). Network Security Vulnerabilities: Malicious Nodes attack. International Journal of Scientific and Research Publications, 4(7), 1-5.
[13] Flowerday, S. V., & Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. computers & security, 61, 169-183.
[14] Yusif, S., & Hafeez-Baig, A. (2021). A conceptual model for cybersecurity governance. Journal of applied security research, 16(4), 490-513.
[15] Pawar, M. V., & Anuradha, J. (2015). Network security and types of attacks in network. Procedia Computer Science, 48, 503-506.
[16] Tourani, R., Misra, S., Mick, T., & Panwar, G. (2017). Security, privacy, and access control in information-centric networking: A survey. IEEE communications surveys & tutorials, 20(1), 566-600.
[17] Sun, J. (2022). Computer network security technology and prevention strategy analysis. Procedia Computer Science, 208, 570-576.
[18] Bansal, B., Jenipher, V. N., Jain, R., Dilip, R., Kumbhkar, M., Pramanik, S., ... & Gupta, A. (2022). Big data architecture for network security. Cyber security and network security, 233-267.
[19] Ataelmanan, S. K. M., & Ali, M. A. H. (2021). Develop an effective security model to protect wireless network. International Journal of Computer Science & Network Security, 21(3), 48-54.
[20] Almohri, H. M., Watson, L. T., Yao, D., & Ou, X. (2015). Security optimization of dynamic networks with probabilistic graph modeling and linear programming. IEEE Transactions on Dependable and Secure Computing, 13(4), 474-487.
[21] Zhimin Li, Weidong Zhu, Yong Wu & Zihao Wu. (2024). Research on information fusion of security analysts' stock recommendations based on two-dimensional D-S evidence theory. North American Journal of Economics and Finance,74,102261-102261.
[22] Kaiyi Zhao, Pinle Qin, Saihua Cai, Ruizhi Sun, Zeqiu Chen & Jiayao Li. (2024). A generalized weighted evidence fusion algorithm based on quantum modeling. Information Sciences,683,121285-121285.
[23] Olabanji O. M & Ogungbuji S. A. (2024). An Appraisal of the Design Sustainability of Solar Water Heating Systems Via Cosine Similarity Index. Asian Journal of Advanced Research and Reports,18(9),118-135.