J. COMBIN. MATH. COMBIN. COMPUT. 123 (2024) 325–342

Journal of Combinatorial Mathematics
and Combinatorial Computing
www.combinatorialpress.com/jcmcc

Combinatorial Press

Research on Network Security Threat Identification and Defence Strategies Based on Big Data Models

Tianyu Li[1,✉]

[1] *Carey Business School, Johns Hopkins University, District of Columbia, 20001, Washington, United States of America*

ABSTRACT

The core of financial institutions' big data lies in risk control, making network security threat identification essential for enhancing data processing and service levels. This study applies the principles of network information transmission security prevention, combining frequency domain analysis and distributed processing to extract threat characteristics. A financial network security threat identification model is developed using BiGRU and Transformer models, and a SQLIA defense system is constructed by integrating multi-variant execution and SQL injection attack prevention. Additionally, an intelligent network security defense strategy is formulated based on finite rationality theory. Simulation results show an F1 composite score of 90.78% for threat identification, and the STRIPS-BR defense strategy reduces relative risk by 74.81% during peak times compared to other strategies. Supported by big data, this system ensures secure data transmission and enhances the network service capabilities of financial institutions.

Keywords: Frequency domain analysis, BiGRU, Transformer, SQLIA defense, Network security threat identification

1. Introduction

In the context of big data, the occurrence of financial risks is closely related to financial information, and the improper use of financial users' personal information can cause many problems. Finance is the core of the modern economy, the financial market is the artery of the whole market economic system, for financial institutions and the financial industry, the degree of security of financial information is

✉ Corresponding author.
E-mail addresses: tli110@jh.edu (Tianyu Li).

Received 19 June 2024; accepted 20 August 2024; published 31 December 2024.

DOI: 10.61091/jcmcc123-23

closely related to the dilemma. Financial information security dilemma is the result of large-scale accumulation of risk, which is the extreme caused by financial information insecurity [24, 1, 11, 29].

Big data finance refers to financial services utilizing big data technology, which can promote financial institutions to launch new financial products and financial services, deeply mine financial users' personal information and private data, and provide means for financial institutions to carry out financial innovation and develop high-value commodities [7, 8, 20, 16]. However, with the continuous development of social economy, big data finance has also triggered new security dilemmas while providing convenience for people's daily life. Financial institutions recklessly collect, store, and use user data information, leading to a sharp rise in the risk of telecommunication fraud and account theft [14, 9, 22, 2]. In response to issues such as the risk of financial information security in the big data environment, users often generally lack sufficient awareness. And due to the users' neglect of the value of financial information itself, they may further ignore the privacy risks that may arise in the process of financial information management, especially based on the use of big data technology [27, 6, 19, 21]. Therefore, it is very necessary to rationally reveal and clearly analyze the financial information security problems, provide corresponding countermeasures and reflections and build an information security system [28].

Literature [3] emphasizes that the development of technology has created opportunities and challenges for the financial sector, which is currently facing cyber threats such as data breaches. The props used by the group of cyber attacks were studied to reveal the basic framework of cyber attacks and the impact it has on financial institutions. Literature [25] states that an important factor to consider in using big data is privacy security. The possible security issues are discussed using a banking institution that has adopted the BeiDou system as a case study, and the results of the experiment are complementary to the current research areas of big data and information security, in addition to being able to provide a reference for the development of security strategies for enterprises in the big data environment. Literature [23] designed a series of interview questions with Canadian cybersecurity professionals in the context of financial institutions facing significant security risks. The results of the interviews confirmed the potential threat posed by cyberattacks to the financial sector, and the researchers made policy recommendations accordingly. Literature [10] suggests that protecting data without being compromised is important in the cyber age, and the use of machine learning, biometrics, and data learning can prevent data from being compromised. For banks, methods such as biometrics and digital signatures can ensure the security of transactions and reduce threats to the banking system. Literature [18] indicates that the increasing reliance on artificial intelligence to process financial data has led to rising data security issues. Research has shown that the application of AI in big data management can effectively improve the security and privacy of AI in the financial industry, while at the same time increasing the attacks from complex networks. Literature [17] states that financial data protection has become a very important issue in the context of technological development. The challenges to cyber security and the effectiveness of existing protection measures were analyzed. The results show that cyber threats have a complexity that cannot be addressed by existing security measures, which requires financial institutions to adopt more effective defense measures. Literature [30] found that due to the interconnectedness of the financial sector and the promotion of coordinated regulation, a more unified standard for cybersecurity is gradually being developed globally, and even though there are still differences in aspects such as data protection, combating cyberthreats requires international cooperation and information sharing. Literature [4] emphasizes that any damage caused to a bank has the potential to affect the entire economic landscape, so the management of cyber threats becomes very important. The financial threats faced

by banks and other financial institutions are analyzed and the techniques as well as strategies to counter the threats are discussed. Literature [5] illustrates that the continuous development of banks in the digital era highlights the importance of cyber security measures. The aim of the study is to provide feasible recommendations for cybersecurity risks in banks to cope with the complex digital risks faced by banks and thus ensure the security of the financial sector.

Everything has two sides, the Internet in equality, efficiency, transparency and other advantages of the other side, is the emergence of endless information security problems, let alone will become a potential network security threats. This paper starts from the principle of financial institutions network information transmission security prevention, through the financial institutions situational awareness platform for network security data processing, and combined with frequency domain analysis and distributed processing to obtain the characteristics of financial institutions network security threats. The BiGRU model is used to learn the local dependencies of cybersecurity threat feature data, and the long-distance dependencies in sequence data are captured by the Transformer model, so as to establish a cybersecurity threat identification model for financial institutions. Based on the consideration of SQL injection attack, the SQLIA defense system is constructed for defending financial institutions' cybersecurity threats by combining with multivariate execution. An intelligent planning method for cybersecurity defense strategy is designed through the theory of finite rationality to obtain a defense strategy that better meets the cybersecurity threats of financial institutions, thus enhancing the defense capability of financial institutions against cybersecurity threats.

2. Cyber Information Transmission and Threat Characteristics of Financial Institutions

The attributes of financial products and services are particularly suitable for publicizing, promoting, selling and servicing through the Internet - this is one of the foundations on which the financial Internet and Internet finance industry have been able to gain rapid development in recent years. Both Internet finance and financial Internet are utilizing the advantages of Internet technology in the collection, storage and processing of information to improve the processing efficiency of financial big data, which can enhance the ability to identify cybersecurity threats, the ability to control risks and the level of pricing, as well as provide customers with more convenient and affordable services.

2.1. Network information transmission security prevention principle

In the big data environment, due to the large amount of data in financial institutions, the scope of data transmission security prevention must be expanded in order to effectively prevent invasive behavior, and to resist invasive behavior by means of active prevention. Based on the distribution characteristics of the information nodes in the financial network, the prevention system is set up so that it covers each intrusion attack node. If the information in a node is found to be invaded and attacked, an alarm is immediately issued, thus providing active defense [15].

According to the characteristics of financial network data, construct a data intrusion attack antigen set (a collection of elements to resist intrusion attacks), labeling parameters such as protocol types, ports, and IP addresses. According to the different access behaviors, the user access behaviors are split into two subsets. One subset is used to store normal access behavior and the other subset is used to store abnormal access behavior. Affinity is used as a tool for active defense against intrusion and two cases are set, in case of this threshold value is 1, it is considered that active defense is

possible and if this threshold value is 0, it is considered that intrusion behavior cannot be effectively prevented. The threshold model is as follows:

$$f_{match}(x,y) = \begin{cases} 1, & \left(f_{h\_dis}(x,y)/l\right) \geq \theta, \\ 0, & \text{otherwise}, \end{cases} \tag{1}$$

where $f_{h\_dis}(x,y)$ represents the clone (access behavior) affinity (an indicator reflecting the characteristics of the antibody, which in this paper refers to the ability to defend against invasive behavior), $f_{match}(x,y)$ represents the monoclonal antibody affinity, and l represents the character string.

In order to effectively prevent invasive behavior, there must be enough antibodies, and when the number of antibodies reaches a certain value, it can provide a good defense effect. However, some of the antibodies in the prevention process will be affected by the environment and other factors, resulting in the death of the antibody, the number of changes and so on. The number of antibodies in the defense system has the characteristic of dynamic change, flowing in from one side and out from the other. The dynamic set of immature antibodies can be expressed as:

$$I(t+\Delta t) = I(t) + \Delta t - \left(\frac{\partial I_{mature}}{\partial x_{mature}} + \frac{\partial I_{dead}}{\partial x_{dead}}\Delta t\right), \tag{2}$$

where $\frac{\partial I_{matures}}{\partial x_{mature}}$ represents the inflow process and $\frac{\partial I_{dead}}{\partial x_{dead}}$ represents the outflow process. The superposition of the number of antibodies of the two processes is the total number of antibodies in the current set. Eq. (2) is utilized to describe the number of data invasive behaviors in a given time domain range.

In the process of using antibodies to defend against invasive behaviors, the tolerance of antibodies is required to be high. By activating the memory antibody, the antibody is made to shift from immature to mature state to defend against the invasive behavior. In this case, the behavior is an active behavior, which actively defends against the invasive behavior within the threshold of activation. The formula for the transformation of antibody properties is as follows:

$$\frac{\partial M_{active}}{\partial X_{active}}\Delta t = \frac{\partial T_{active}}{\partial X_{active}}\Delta t, \tag{3}$$

where M_{active} represents mature active antibody, in the activated state, T_{active} represents mature antibody, in the activated state, and X_{active} reaches the standard active antibody.

When an intrusion occurs in the network of the financial institution, the memory antibody is activated, causing the immature antibody to evolve to the mature antibody, which actively recognizes the intrusion and stops the access, protecting the information data in the transmission process, and playing a good preventive role.

2.2. Cybersecurity data processing for financial institutions

For financial institution big data, this paper relies on the financial institutions' situational awareness platform to collect financial massive data, and the data obtained from traffic logs, network devices and other dimensions are analyzed and processed in a complex manner with high real-time and high efficiency. The network security data processing flow of financial institutions is shown in Figure 1, which applies a large number of advanced cutting-edge technologies to support and realize data security analysis and processing capabilities. Among them, Flink is a distributed processing engine for streaming data and batch data, and data processing adopts Flink to process streaming data, adopts Ambari for management and deployment, is compatible with Flink eco-software, and

supports computational models such as SQL, Table, CEP, and machine learning. The situational awareness of big data for financial institutions is based on Apache Flink, a distributed data stream processing system, and Siddhi, a complex event computing engine, with excellent characteristics of high throughput, low latency, high performance and high flexibility.

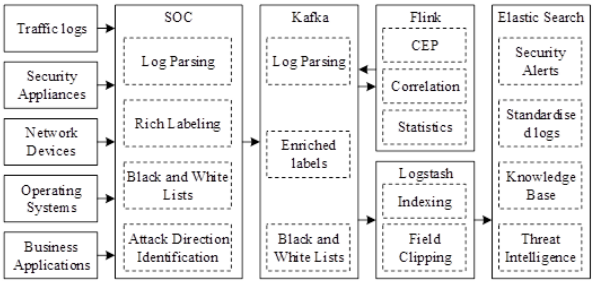


Fig. 1. Network security data processing process

The situational awareness data processing of financial institutions' big data contains various big data-related technologies, which can be configured through security analysis based on the business scenario's statistical model, rule model, correlation model, etc., and perform the calculation of statistics, summation, mean value, unique value and other operators on any field in the data. It can realize high real-time computing of network security in financial service scenarios through the association of event priority and field containment relationship for multi-source data.

2.3. Financial network security threat feature extraction

On the basis of constructing the data processing flow of financial network security information transmission, the threat features of financial institutions' network transmission security are extracted. Combined with the network topology restructuring method to realize the distributed reconstruction of the dynamic features of network transmission information, the dynamic iterative processing of network information transmission is realized according to the combined frequency domain factor distributed fusion technology. This technique combines the combined frequency domain analysis method with distributed processing, analyzes the frequency domain data collected by each node in the network, extracts the frequency domain factors related to network transmission, and passes the analyzed frequency domain factor information to other nodes in the network [26]. Distributed computing and communication are used to realize information exchange and sharing, and dynamic iteration is carried out between nodes to optimize and improve network information transmission by gradually adjusting and optimizing network transmission parameters and strategies through continuous information exchange and updating. The set of principal component feature distribution of all network transmission channels of a particular LAN is obtained as:

$$\min \tfrac{1}{2}\|W\| + C\sum_{j=1}^{t} x(t)\xi_j, \ \text{ such that } \ y_j\left(W \cdot x\left(t\right) + b\left(x\right)\right) + \xi_j \geq 1 \ \ \xi_j \geq 0, j = 1, 2, \cdots, l, \tag{4}$$

where, W is the node weight, C is the suspected attack behavior capacity parameter, ξ_j is the base learner for the jth round of training, each individual learner is independent of each other, and the data collection is performed using self-sampling method in the original training set. The speed of each individual learning in the original training set is $V^i = (v_{i1}, v_{i2}, \cdots, v_{iD})^T$ and the location of the network threat point is $X_i = (x_{i1}, x_{i2}, \cdots, x_{iD})^T$. Threat dynamic parameter analysis is carried out in the original training set using self-service sampling method, and the distribution kernel function of

the base learning for the jth round of training is $k(x_i, x_j)$. Individual base learners are independent of each other and multiple primary individual learning models are obtained as:

$$\min_{\alpha} \frac{1}{2} \sum_{i=1}^{l} \sum_{j=1}^{l} y_i y_j \alpha_i \alpha_j K(x_i, x_j) - \sum_{j=1}^{l} \alpha_j, \text{ such that } \sum_{j=1}^{l} y_j \alpha_j = 0 \ 0 \leq \alpha_j \leq u(x_j) C, j = 1, 2, \cdots, l, \tag{5}$$

where, $K(x_i, x_j)$ is the training kernel function of real attack samples, α_i is the proportion of real attack samples in the dataset that are recognized, α_j is the proportion of real attack samples in the dataset that are not recognized. y_i is the proportion of real attack samples in the dataset that are recognized, y_j is the proportion of real attack samples in the dataset that are not recognized, and $u(x_j)$ is the feature parameter of the jth round of training.

Using the greedy algorithm of fuzzy clustering, the subscript of security threat identification is obtained g_{best}. Judging by the threshold, but less than the threshold indicates the existence of the possibility of attack, at this time, the objective function containing the regular term is obtained as:

$$w_{ij} = \beta w(e_p k_q) + K(x_i, x_j), \beta > 1, \tag{6}$$

where β is the adaptive weighting coefficient of sample x on the decision tree, and $w(e_p k_q)$ denotes the objective function gain, whereby all the values of each feature are traversed through the time gain judgment to obtain the threat characteristics of the network transmission information as:

$$Y_k = w_{ij} [y_{k1}, y_{k2}, \cdots, y_{kj}, \cdots, y_{kj}], k = 1, 2, \cdots, N, \tag{7}$$

where y_{kj} denotes the set of gradient instance data, and N is the data length, from which the feature extraction model is established, and the dynamic detection of network information security threats is carried out based on the feature extraction results.

3. Cybersecurity Threat Identification Model for Financial Institutions

In the new era, the development of technology has brought great influence to the development of financial institutions, and the huge amount of data it generates makes financial institutions pay more and more attention to network security threats, and the application of technology can effectively realize the dynamic identification of network security threats. However, through the analysis of the actual situation, it is found that there are many problems in the identification of network security threats, and the application of technology should be combined with the computer network to avoid network security problems affecting the application and development of technology. Therefore, financial institutions need to deeply explore the threat characteristics of financial data in network transmission, combined with the actual situation of technology application, in order to improve the level of financial institutions services and network security.

3.1. Network security threat recognition model architecture

The overall structure and flow of the financial network security threat recognition model is shown in Figure 2. The design idea of the model proposed in this paper lies in the advantages of financial cybersecurity threat feature selection and data balancing processing, which in turn improves the model's ability to process complex sequence data through the deep integration of Transformer and BiGRU. Compared with existing research, this model has significant differences and advantages in feature optimization, data balancing, and long dependency capturing.

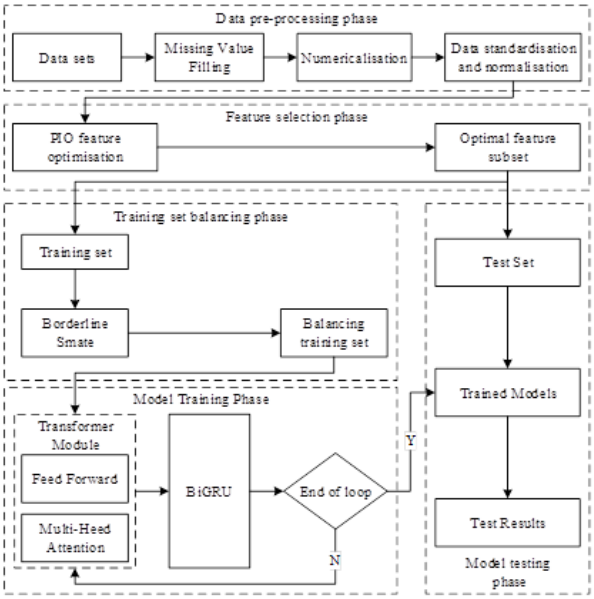


Fig. 2. Model architecture frame

In this paper, we adopt the combined architecture of Transformer + BiGRU, in which Transformer is responsible for capturing long-distance dependencies in sequence data, while BiGRU focuses on learning local dependencies in data and controlling the flow of information through a gating mechanism, so that the model can be more flexible to adapt to different levels of feature representation. This structural design makes the model more accurate and efficient in handling data with complex patterns. The final results are obtained by performing performance tests on the previously trained model using a prepared test set after model training.

The model in this paper has excellent processing capabilities, especially on high dimensional and long sequence data, and achieves high prediction accuracy and efficiency through feature optimization, data balancing and deep neural network integration. Its hybrid architecture strategy not only enhances the flexibility and robustness of the model, but also effectively prevents the overfitting problem and improves the practicality and scalability of the model.

3.2. BiGRU and transformer models

3.2.1. Bidirectional gated recurrent neural network (BiGRU). BiGRU is a structure that uses two unidirectional gated recurrent units.The basic idea of this structure is to process the input sequence in both forward and backward directions at the same time and connect the outputs from both directions to a common output layer.Conventional recurrent neural networks can only utilize the past input information when making predictions.BiGRU will process the input sequence simultaneously in both forward and backward direction of the GRUs for processing. In this case, the forward GRU processes the input sequence in normal chronological order, while the backward GRU processes the input sequence in reverse order. In this way, the hidden state at each moment captures both past and future contextual information [12]. The computational procedure of BiGRU neural network is as follows:

Assuming that the input at time step t is x_i, the activation function of the hidden layer is ∂, and

that the left side of Eq. are the forward and backward hidden states, respectively, then:

$$\overrightarrow{h_t} = \partial\left(x_t W_{fx} + \underset{h_{t-1}}{\rightarrow} W_{fh} + b_{fh}\right), \tag{8}$$

$$\underset{h_t}{\leftarrow} = \partial\left(x_t W_{bx} + \underset{h_{t-1}}{\rightarrow} W_{bh} + b_{bh}\right), \tag{9}$$

where W_{fx}, W_{fh}, W_{bx}, W_{bh} denote the weight parameters, b_{fh}, b_{bh} denote the bias corresponding to the forward hidden state and backward hidden state, respectively. From this, the output GRU_O_t of the output layer is calculated as:

$$GRU\_O_t = \left(\underset{h_t}{\rightarrow} \middle| \underset{h_t}{\leftarrow}\right) \cdot W_q + b_q. \tag{10}$$

The final output is calculated by weighted splicing of forward hidden state and backward hidden state, which can learn the effective information and also keep the output dimension unchanged, which reduces the dimension and helps to reduce the training time compared to directly splicing the hidden state in both directions.

3.2.2. Transformer model. The Transformer model is based on the "encoding-decoding" framework, where the input is word vectors and positional encoding is added after each word vector to prevent semantic confusion [13]. The positional coding is calculated as follows:

$$PE(pos, 2i) = \sin\left(\frac{pos}{10000^{\frac{2i}{dmodel}}}\right), \tag{11}$$

$$PE(pos, 2i+1) = \cos\left(\frac{pos}{10000^{\frac{2i}{dmodel}}}\right), \tag{12}$$

where *pos* denotes the absolute position of the word in the sentence and *dmodel* denotes the dimension of the word vector.

Transformer uses the Multi-Head Attention mechanism, which provides multiple "representation subspaces", allowing the model to attend to information from different "representation subspaces" at different positions, i.e., the model can capture richer feature information through "Multi-Head", the model can capture richer feature information. The Multi-Head attention mechanism is diagrammed and described as:

$$MultiHead(Q, K, V) = Concat(head_1, ..., head_h)W^0, \tag{13}$$

$$head_i = ATT(QW_i^Q, KW_i^K, VK_i^V), \tag{14}$$

where Q denotes the query vector, K denotes the key vector, V denotes the value vector and WQ, WK, WV is the weight.

A residual connection layer is added to each sublayer in the Transformer language model to avoid gradient vanishing. In order to speed up the training of the model and improve the stability of training the input data is normalized and the normalization layer uses the LN algorithm. In the Transformer model, each word vector is computed by the multi-head attention mechanism and then further processed by the feed-forward network to extract richer semantic information.

3.3. Simulation verification of network security threat identification

3.3.1. Comparative experiments on cybersecurity threat recognition. In order to verify the effectiveness of the cybersecurity threat recognition model for financial institution big data designed in this paper, a comparison experiment is set up in this section. The training cluster used is the UNSW_NB dataset with intrusion signals in financial institution big data, and several different algorithms are selected as comparisons, with the evaluation indexes of accuracy rate, precision rate, recall rate and F1 comprehensive score. The cyber security threat recognition results of different models are shown in Table 1.

The accuracy, precision and recall of the model proposed in this paper reached 90.64%, 90.51% and 89.84%, respectively, and the F1 score reached 90.78%, which achieved relatively good results in all the evaluation indexes. This is because traditional machine learning methods are easily affected by irrelevant and redundant features, so the performance of the model is still not as good as the deep learning model. In this paper, the model learns features through neural networks, combines low-level features to form a more abstract and nonlinear high-level representation, and then utilizes the input-output relationship between the data to effectively improve the accuracy of cybersecurity intrusion detection of financial institutions' big data, and combines the BiGRU and Transformer models, which can better mine the security threat features in financial institutions' big data. Compared with the existing VAE-CWGAN, MCNN-DFS, GAN-BiLSTM, SSAE-LSTM, CNN-GRU, and CNN-BiLSTM models, the BiGRU network in this paper's model fully combines the advantages of the GRU network, improves the problem of the gradient vanishing, and constructs a deeper network structure, extracts more complex and abstract features. Subsequently, the Transformer model is utilized to improve the feature learning ability of cyber security threats, thus solving the problem of insufficient feature extraction ability of the model. The method in this paper has great improvement for the aspects of high dimensionality of features, imbalance of dataset and single model, and has higher accuracy in identifying few attack traffic in financial institutions' networks, and these good experimental results further prove the effectiveness of this paper's model.

Model	Accuracy	Precision	Recall	F1-score
RF	78.97	75.04	81.15	79.42
SVM	78.35	75.72	78.87	73.51
KNN	80.51	77.63	77.65	77.84
VAE-CWGAN	89.03	88.51	88.57	88.38
MCNN-DFS	82.87	81.42	81.02	81.42
GAN-BiLSTM	89.25	85.79	85.72	85.51
SSAE-LSTM	87.66	83.75	71.98	82.97
CNN-GRU	83.08	8563	86.18	83.48
CNN-BiLSTM	88.03	85.72	84.75	85.92
Ours model	**90.64**	**90.51**	**89.84**	**90.78**

Table 1. Network security threat recognition results (%)

3.3.2. Network security posture analysis of financial institutions. The network security posture analysis of financial institutions takes the attack as the starting point, selects 10 minutes as a time window, and calculates the security posture change values of different services, different

hosts, and networks in a hierarchical manner, reflecting the occurrence of network attacks in the time window by analyzing the sudden change of the security posture values in each time window. Three hosts with IPs 192.168.126.12, 192.168.126.14, and 192.168.126.16 are selected as the research objects, which are named Client1∼Client 3 respectively, and the network security posture of the three hosts is analyzed. Figure 3 shows the results of network security posture analysis, in which Figure 3(a) shows the posture graphs of the three services of DNS, HTTP and SMTP in Client1, and Figure 3(b) and (c) show the posture changes in the host layer and network layer, respectively.

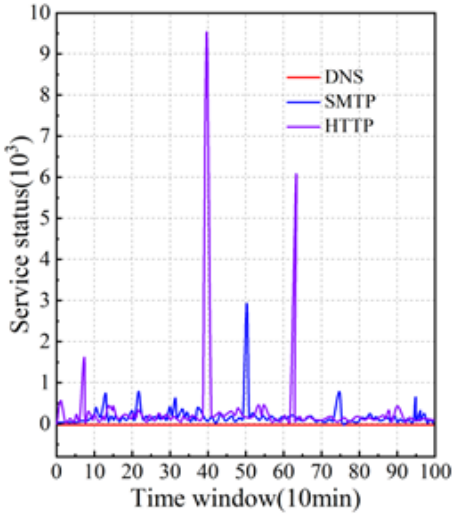
(a) In the security posture results of the service layer, the host has high service posture values for HTTP service in the 38th-42nd time windows as well as in the 60th-65th time windows, and has been subjected to a single large-scale and larger-scale attack, which requires the financial institution to pay special attention to it. The SMTP service was attacked once on a small scale in the time window 49-51, in addition to which the HTTP and SMTP services were attacked several times on a smaller scale. Financial institutions need to make appropriate protective measures based on the network security posture of financial services.

(b) In the results of the security posture at the host layer, Client1 suffered a small-scale attack in the 10th time window, a larger-scale attack in the 59th to 62nd and 93rd to 95th time windows, and many times suffered from small-scale attacks; Client2 suffered a large-scale attack in the 10th and 71st to 75th time windows, a large-scale attack in the 31st to 33rd time windows, and many times suffered from small-scale attacks. ∼Client3 suffered one large-scale attack in the 10th-13th, 28th-32nd, and 48th-52nd time windows, and many minor attacks in the rest of the time. Based on the results of the cybersecurity posture of financial hosts, skill organizations need to pay more attention to hosts with high attack threat indexes.

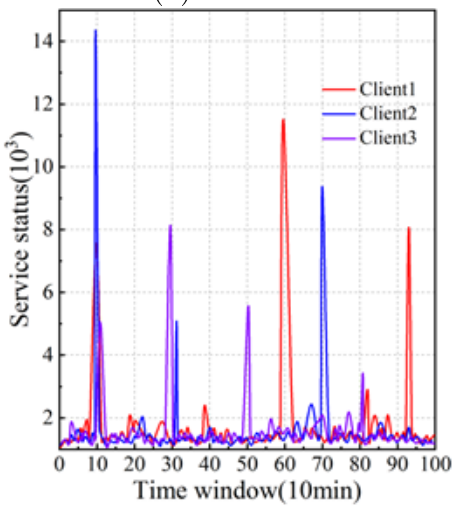
(c) In the security posture results of the network layer, the network suffered a large-scale attack in the 20th to 22nd and 52nd time windows, and suffered large-scale attacks and small-scale attacks several times. This figure can reflect the security status of the network correctly and help financial institutions to monitor the security status of the network. Financial institutions should survey and protect the network according to the posture figure, and pay attention to the information of users who accessed the network in the 20th-22nd and 52nd time windows, so as to confirm the malicious access users and take appropriate measures in this regard.

4. Cybersecurity Defense Strategy Options for Financial Institutions

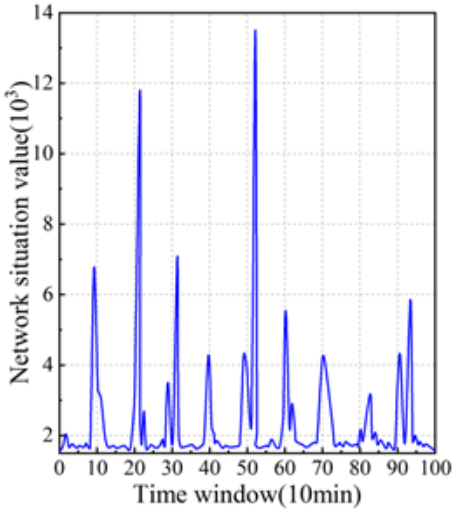
In the context of the development of the era of big data, computer network technology has been widely used in the financial field, so the network security and stability of financial institutions has put forward higher development requirements. As an important carrier of information technology and network technology, computer network carries the security defense of the entire financial network, and once the network is maliciously attacked, individuals and other private data information will be seriously affected, and even endanger the safety of life. Deep learning technology as an intelligent emerging technology, has a strong robustness and stability, its application to the network security defense of financial institutions, can effectively improve the overall security performance of the network, to avoid malicious attacks on the network.



(a) Client1



(b) Host posture



(c) Network posture

Fig. 3. Network security situation analysis results

4.1. SQLIA defense based on multivariate execution

Most of the multi-variant execution architectures use Leader-Follower or Master-Slave design, for the system calls that are not voted, the monitor assigns them to the Leader/Master variant for execution, and then synchronizes the results to the Follower/Slave variant, this approach can effectively reduce the false positives, but it increases the security threats [31]. Once the Leader/Master variants are controlled, the defense effectiveness of the multivariate execution architecture will be greatly reduced. In this paper, we propose the SQLMVED network security defense architecture based on multivariate execution as shown in Figure 4. To avoid the security threat of Leader-Follower/Master-Slave mode, synchronous mode is used, and the system consists of a user request agent, a multivariate responsible for processing the request, a database agent, and a database.

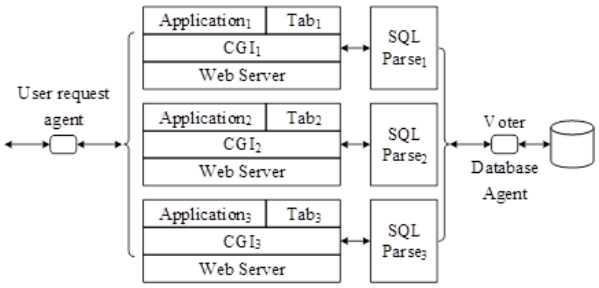


Fig. 4. SQLMVED network security defense architecture

The user request agent is the gateway to the web service, when it receives a request initiated by the user, it makes three copies of the request and forwards them to the multivariate. When it receives a response from a multi-variant, it votes on it, and if there is a unanimous majority response, it returns it to the user, otherwise it rejects the response. The user request broker is based on the Nginx implementation, which realizes the forwarding of the same user's request to multiple variants and the voting of the same user's response. The multi-variants consist of a web server, a CGI, and a deployed application, where the application uses a randomization method to randomize changes to the SQL, and the labels used are different between the variants. The database agent consists of a SQL syntax parser, SQLParse, which serves each variant independently, and a voting agent that compares the results of its parsing.The SQL syntax parser is based on the sqlparse/keywords.py file, which aligns the tokens.Keyword with the randomization labels, and completes the process of parsing the randomized SQL and de-randomizing it.

4.2. Intelligent planning for cybersecurity defense strategies

Intelligent planning aims to achieve desired goals by executing a series of actions. By using it in the cyber security defense scenario of financial institutions, it can simulate the human defense behavior, focus on the current urgent defense measures of the system, and reach the target state by executing a series of defense strategies from the initial state, so as to achieve the cyber security defense goal.

In this paper, considering the advantages of the finite rationality method in supporting the selection of cyber defense strategies for financial institutions, we set the boundary conditions of time, cognition and information, expand the STRIPS language finite rationality to STRIPS-BR, intelligently allocate resources within the scope of finite rationality, plan the best current cybersecurity defense scheme and automate its implementation, so as to realize the asset security goal.

STRIPS-BR first defines three constraints in finite rationality, i.e., time-limited, cognitively limited, and information-limited. Among them, time-limited $BR-A(T)$ and cognitively limited $BR-A(C)$

can be judged by checking whether the time count and cognitive depth of the state have exceeded their respective limits, respectively, and information-limited $BR-A(I)$ includes unknown or incorrectly assumed asset states $S-BR$, goal propositions $G-BR$, and available finite defense strategies CM-BR. Based on this information, we build a search tree to obtain all the planning scenarios that can satisfy the goal state P^x. The defense strategy in P^x Sequential execution results in O^x and $rank(s_i)$ is the actual sequence of defense strategies executed.

To determine the optimal (highest utility) defense planning scheme, define $U\left(P_{0,k}^x\right)$ as the cumulative planning utility of the defense strategies from the beginning to the kth defense strategy in planning P^x, i.e:

$$U\left(P_{0,k}^x\right)=\sum_{t=0}^{k} w_t^x, \tag{15}$$

where w_k^x is the weight of the krd defense strategy cm_k^x in P^x, i.e:

$$w_k^x = in-\deg ree+0.1\sum_v cvss_v+\lambda, \tag{16}$$

$$cvss_v=\alpha CVSS_v, \tag{17}$$

where in-degree is the in-degree of defense strategy cm_k^x, $cvss_v$ is the product of the probability α of adopting defense strategy cm_k^x against vulnerability v and the CVSS score of vulnerability v, and $\sum_v cvss_v$ is the sum of the $cvss_v$ values of the existing vulnerabilities v that can be solved by executing the defense strategy cm_k^x reflecting the importance of the strategy for the existing vulnerabilities. λ is a correlation factor representing the correlation between the current defense strategy cm_k^x and the previous one, $\lambda=0.3$ if the current defense strategy is related to the previous one (belonging to the same security means), and $\lambda=0$ otherwise.

4.3. Validation of the effectiveness of network security defense

4.3.1. Comparison of financial service system risks under different strategies. In this paper, the request traffic transmitted by financial institutions is divided into four different request traffic intensity levels: the "low peak period" from 0:00 to 5:00, the "peak period" from 6:00 to 11:00, the "peak period" from 12:00 to 17:00, and the "burst period" from 18:00 to 23:00. This paper proposes a SQLIA defense system based on multi-variant execution, and uses the STRIPS-BR defense strategy to defend against network security threats in financial institutions. In order to measure the defense effect of the STRIPS-BR strategy on the financial service system, the relative risk value of the successful attack of the system when the financial service system adopts different defense strategies for system dynamic configuration is shown, as shown in Figure 5.

Comparison of the results shows that STRIPS-BR reduces the system risk value relative to other strategies by 22.68%, 48.57%, 74.81% and 41.54% on average during the low-peak, flat-peak, peak and outbreak periods, respectively, which indicates that STRIPS-BR has a stronger financial services network security defense capability. With the arrival of the traffic outbreak period, the advantage of STRIPS-BR is more obvious, which shows that the STRIPS-BR defense policy for financial services network resource allocation and defense configuration intelligent planning for integrated decision-making can better respond to the changes in the request traffic. financial services under the DSEOM policy has the largest system risk value, which is mainly due to the fact that the DSEOM targets critical financial services for The main reason is that DSEOM protects against critical financial services, and there is a possibility that attackers bypass critical financial services to intrude into critical data

nodes, so the financial service system risk assessment under this strategy has a poor performance.The SmartSCR strategy has a significant security improvement compared to the DSEOM strategy, because the SmartSCR strategy improves the security of the financial service system by providing protection for all financial services. The reason for the better defense effect of STRIPS-BR is that it takes into account the security gain of the financial service system by the randomization of replicas introduced in the resource allocation process, so that the security of the financial service system can be further strengthened by the targeted resource allocation under the dynamic user traffic.

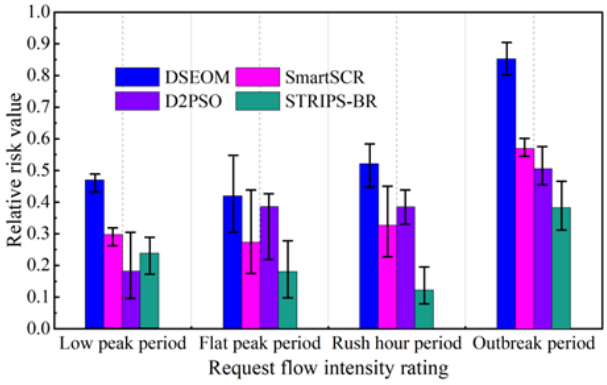


Fig. 5. The risk comparison of financial services in different strategies

4.3.2. Network security threat defense performance. Based on the SQLIA defense system executed by multi-variants, combined with the results of network security threat identification, a network security defense strategy based on STRIPS-BR is designed. In order to further verify the effectiveness of the strategy's network security threat defense, this paper takes the proportion of passage through normal traffic (PA) and the proportion of passage through malicious traffic (PB) as the evaluation indexes, and obtains the results of the effectiveness of the financial institution's network security threat defense as shown in Figure 6.

As can be seen from the figure, after 10 rounds, the proportion of attack traffic reaching the target host is stabilized at 25%, and the proportion of legitimate traffic reaching the target host is maintained at about 75%, which indicates that the financial institution network security defense strategy based on STRIPS-BR plays an obvious mitigation effect on flooding attack traffic, and it can compress the passage rate of malicious traffic as much as possible, while reducing the impact on legitimate traffic to ensure that the network bandwidth resources are not occupied by malicious traffic.

5. Optimization of Cybersecurity Defence Strategies for Financial Institutions

Under the environment of unpredictable cyber shock, cyber security has been the focus of extensive attention from both theoretical and practical circles in recent years. And finance, as the weathervane of a country's economy, is the industry most vulnerable to cyber siege. Whether it is risk management, bookkeeping and clearing, or asset pricing and digital currency, the financial industry's network construction has been in the forefront of all industries. Under the existing big data environment of financial institutions, it is crucial to ensure the secure transmission of financial institutions' networks and improve their ability to identify and defend against cybersecurity threats.

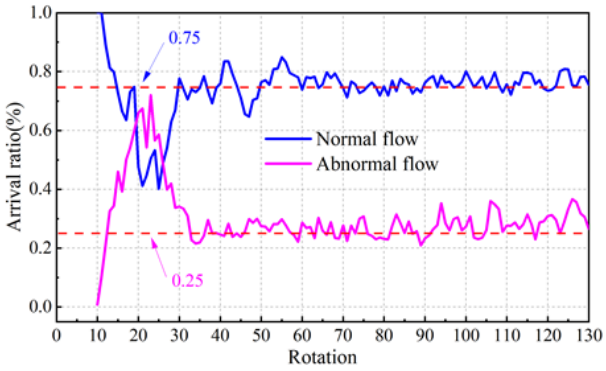


Fig. 6. Network security threat defense effectiveness results

5.1. Constructing a network security threat defense system

5.1.1. Financial institutions need to understand highly sophisticated attack activities. The asset security operation and maintenance platform is used to clarify the asset base, form the network and air topography, and establish a unified security patch and unified security policy distribution and adjustment system to realize effective asset security reinforcement. Through effective data collection and intelligence production on the endpoint side, network side and analysis side, we build a situational awareness platform system and conduct data aggregation and analysis to form effective security policies.

5.1.2. Threat insight, systematic planning, and effective protection. Financial institutions must face up to the security challenges brought about by open scenarios and the growth in the scale of information systems, comprehensively improve network security planning capabilities, and implement full life cycle security planning, construction, operation and maintenance. Important information assets and large-scale information assets need to be set up with the objective enemy situation of "the enemy is already inside and the enemy will be inside". With reference to the "threat framework", we should update our systematic knowledge of threat actors and attack activities, so as to deepen and improve the setting of the hostile situation and thus improve defense.

5.2. Financial services security threat response strategies

With escalating cyber threats and increased regulatory demands, it is imperative for financial institutions to establish a comprehensive cyber security response strategy to protect their systems and entrusted data from cyber attackers.

(a) Establish a reliable access management strategy. Key components of an access management strategy include cloud access security agents, multiple authentication, privileged access management, and zero-trust network access. Cloud access security proxy solutions monitor and manage access to an organization's cloud-based applications, and multiple authentication requires users to authenticate to an account using a combination of multiple factors, such as passwords and physical tokens. Privileged access management solutions are critical for accounts with higher access rights to monitor and manage sensitive systems and data, and zero-trust network access can enable financial institutions to manage data security risks and meet regulatory compliance requirements by providing access to data.

(b) Ensure endpoint security and user safety and trust. One is Extended Detection and Response,

a solution designed to take a more holistic approach to detecting and remediating threats by collecting data from multiple sources (endpoints, email, network traffic, etc.) and analyzing it to identify these attacks. The second is the Secure Web Gateway, which sits between users and the Internet and proxies all connections, enabling organizations to block access to inappropriate or dangerous sites and monitor for malicious content.

6. Conclusion

The article uses frequency domain analysis and distributed processing to extract the cyber threat features of financial institutions, establishes a cyber security threat identification model by combining BiGRU and Transformer model, then establishes a SQLIA defense system based on multi-variant execution, and designs a STRIPS-BR strategy for cyber security threat defense of financial institutions. The comprehensive score of F1 for cybersecurity threat identification of financial institutions based on BiGRU and Transformer model can reach 90.78%, which can effectively analyze the cybersecurity posture of financial institutions under different network layers. The relative risk value obtained by the STRIPS-BR strategy based on intelligent planning of cybersecurity defense strategies is 41.54% lower than that of other strategies during the outbreak period, which can suppress the abnormal traffic of the financial network at about 25%. Financial institutions need to establish a network security threat and defense system, which is carried out in the dimensions of access management policy, endpoint security and user security, so as to ensure the improvement of the security level of financial institutions' services.

References

[1] E. D. Borghard. *Protecting financial institutions against cyber threats: A national security issue*. JSTOR, 2022.

[2] D. L. Coss, K. Smith, J. Foster, and S. Dhillon. Big data in auditing: a value-focused approach to cybersecurity management. *Journal of Information Systems Security*, 15(2), 2019.

[3] N. T. Cyriac and L. Sadath. Is cyber security enough-a study on big data security breaches in financial institutions. In *2019 4th International Conference on Information Systems and Computer Networks (ISCON)*, pages 380–385. IEEE, 2019. https://doi.org/10.1109/ISCON47742.2019.9036294.

[4] A. A. Darem, A. A. Alhashmi, T. M. Alkhaldi, A. M. Alashjaee, S. M. Alanazi, and S. A. Ebad. Cyber threats classifications and countermeasures in banking and financial sector. *IEEE Access*, 11:125138–125158, 2023. https://doi.org/10.1109/ACCESS.2023.3327016.

[5] S. O. Dawodu, A. Omotosho, O. J. Akindote, A. O. Adegbite, and S. K. Ewuga. Cybersecurity risk assessment in banking: methodologies and best practices. *Computer Science & IT Research Journal*, 4(3):220–243, 2023. https://doi.org/10.51594/csitrj.v4i3.659.

[6] B. Dupont. The cyber-resilience of financial institutions: significance and applicability. *Journal of cybersecurity*, 5(1):tyz013, 2019. https://doi.org/10.1093/cybsec/tyz013.

[7] A. S. Edu, M. Agoyi, and D. Agozie. Digital security vulnerabilities and threats implications for financial institutions deploying digital technology platforms and application: fmea and ftopsis analysis. *PeerJ Computer Science*, 7:e658, 2021. https://doi.org/10.7717/peerj-cs.658.

[8] O. Efijemue, C. Obunadike, E. Taiwo, S. Kizor, S. Olisah, C. Odooh, and I. Ejimofor. Cybersecurity strategies for safeguarding customers data and preventing financial fraud in the united states financial sectors. *International Journal of Soft Computing*, 14(3):10–5121, 2023. http://dx.doi.org/10.5121/ijsc.2023.14301.

[9] R. P. França, A. C. B. Monteiro, R. Arthur, and Y. Iano. The fundamentals and potential for cybersecurity of big data in the modern world. *Machine intelligence and big data analytics for cybersecurity applications*:51–73, 2021. https://doi.org/10.1007/978-3-030-57024-8_3.

[10] D. Ghelani, T. K. Hua, and S. K. R. Koduru. Cyber security threats, vulnerabilities, and security solutions models in banking. *Authorea Preprints*, 2022. https://doi.org/10.22541/au.166385206.63311335/v1.

[11] A. Gołębiowska, W. Jakubczak, D. Prokopowicz, and R. Jakubczak. Cybersecurity of business intelligence analytics based on the processing of large sets of information with the use of sentiment analysis and big data. *European Research Studies Journal*, 24(4), 2021. http://dx.doi.org/10.35808/ersj/2631.

[12] Z. Jiang, Q. Tan, N. Li, J. Che, and X. Tan. A novel bigru multi-step wind power forecasting approach based on multi-label integration random forest feature selection and neural network clustering. *Energy Conversion and Management*, 319:118904, 2024. https://doi.org/10.1016/j.enconman.2024.118904.

[13] Y. Kurata, M. Nishio, Y. Moribata, S. Otani, Y. Himoto, S. Takahashi, J. Kusakabe, R. Okura, M. Shimizu, K. Hidaka, et al. Development of deep learning model for diagnosing muscle-invasive bladder cancer on mri with vision transformer. *Heliyon*, 10(16), 2024. https://doi.org/10.1016/j.heliyon.2024.e36144.

[14] Y. Liu. Development and risk of internet finance based on big data. In *Cyber Security Intelligence and Analytics: 2021 International Conference on Cyber Security Intelligence and Analytics (CSIA2021), Volume 1*, pages 518–525. Springer, 2021. https://doi.org/10.1007/978-3-030-70042-3_75.

[15] A. Manowska, M. Boros, M. W. Hassan, A. Bluszcz, and K. Tobór-Osadnik. A modern approach to securing critical infrastructure in energy transmission networks: integration of cryptographic mechanisms and biometric data. *Electronics*, 13(14):2849, 2024. https://doi.org/10.3390/electronics13142849.

[16] E. Mwasiaji. Big data security concerns and commercial banks' financial management practices as business intermediaries: the call for a theoretical model. *International Journal of Arts and Commerce, 8 (11), 31-44. ISSN 1929*, 7106, 2019.

[17] C. C. Okoye, E. E. Nwankwo, F. O. Usman, N. Z. Mhlongo, O. Odeyemi, C. U. Ike, et al. Securing financial data storage: a review of cybersecurity challenges and solutions. *International Journal of Science and Research Archive*, 11(1):1968–1983, 2024. http://dx.doi.org/10.30574/ijsra.2024.11.1.0267.

[18] S. O. Olabanji, O. B. Oladoyinbo, C. U. Asonze, T. O. Oladoyinbo, S. A. Ajayi, and O. O. Olaniyi. Effect of adopting ai to explore big data on personally identifiable information (pii) for financial and economic data transformation. *Available at SSRN 4739227*, 2024. https://dx.doi.org/10.2139/ssrn.4739227.

[19] O. P. Olaiya, T. O. Adesoga, A. Ojo, O. D. Olagunju, O. O. Ajayi, and Y. O. Adebayo. Cybersecurity strategies in fintech: safeguarding financial data and assets. *GSC Advanced Research and Reviews*, 20(1):050–056, 2024. https://doi.org/10.30574/gscarr.2024.20.1.0241.

[20] A. E. Omolara, A. Jantan, O. I. Abiodun, M. M. Singh, M. Anbar, and D. Kemi. State-of-the-art in big data application techniques to financial crime: a survey. *International Journal of Computer Science and Network Security*, 18(7):6–16, 2018.

[21] A. T. Oyewole, C. C. Okoye, O. C. Ofodile, and C. E. Ugochukwu. Cybersecurity risks in online banking: a detailed review and preventive strategies applicatio. *World Journal of Advanced Research and Reviews*, 21(3):625–643, 2024. http://dx.doi.org/10.30574/wjarr.2024.21.3.0707.

[22] S. Petrenko. *Big Data Technologies for Monitoring of Computer Security: A Case Study of the Russian Federation*. Springer, 2018.

[23] P.-L. Pomerleau and D. L. Lowery. Countering cyber threats to financial institutions. In *A Private and Public Partnership Approach to Critical Infrastructure Protection*. Springer, 2020. http://dx.doi.org/10.1007/978-3-030-54054-8.

[24] M. A. Rassam, M. Maarof, A. Zainal, et al. Big data analytics adoption for cybersecurity: a review of current solutions, requirements, challenges and trends. *Journal of Information Assurance & Security*, 12(4), 2017.

[25] K. A. Salleh and L. Janczewski. Security considerations in big data solutions adoption: lessons from a case study on a banking institution. *Procedia Computer Science*, 164:168–176, 2019. https://doi.org/10.1016/j.procs.2019.12.169.

[26] K. Saminathan, S. T. R. Mulka, S. Damodharan, R. Maheswar, and J. Lorincz. An artificial neural network autoencoder for insider cyber security threat detection. *Future Internet*, 15(12):373, 2023. https://doi.org/10.3390/fi15120373.

[27] P. Sharma and S. Barua. From data breach to data shield: the crucial role of big data analytics in modern cybersecurity strategies. *International Journal of Information and Cybersecurity*, 7(9):31–59, 2023.

[28] M. Singh, M. N. Halgamuge, G. Ekici, and C. S. Jayasekara. A review on security and privacy challenges of big data. *Cognitive Computing for Big Data Systems Over IoT: Frameworks, Tools and Applications*:175–200, 2018. https://doi.org/10.1007/978-3-319-70688-7_8.

[29] R. Skyrius, G. Giriūnienė, I. Katin, M. Kazimianec, and R. Žilinskas. The potential of big data in banking. *Guide to Big Data Applications*:451–486, 2018. https://doi.org/10.1007/978-3-319-53817-4_17.

[30] N. S. Uzougbo, C. G. Ikegwu, A. O. Adewusi, et al. Cybersecurity compliance in financial institutions: a comparative analysis of global standards and regulations. *International Journal of Science and Research Archive*, 12(1):533–548, 2024. http://dx.doi.org/10.30574/ijsra.2024.12.1.0802.

[31] A. Zhu and W. Q. Yan. Exploring defense of sql injection attack in penetration testing. *International Journal of Digital Crime and Forensics (IJDCF)*, 9(4):62–71, 2017. https://doi.org/10.4018/IJDCF.2017100106.