Update Algorithm of Secure Computer Database Based on Deep Belief Network

Liusuo Huang[1,2,*] and Yan Song[1,2]

[1]*Software College, Henan Finance University, Zhengzhou Henan 450046, China*
[2]*Research Center for Digital Humanities, Henan Finance University, Zhengzhou Henan 450046, China*
E-mail: liusuo_hua12@yahoo.com
[*]*Corresponding Author*

Received 04 November 2022; Accepted 14 December 2022;
Publication 05 December 2023

Abstract

In order to ensure the security of large-scale data transmission in a short time and in a wide range during online database updating, this paper presents a secure computer database updating algorithm based on DBN (Deep Belief Network). In this paper, the model adopts multi-layer depth structure for unsupervised feature learning, maps high-dimensional and nonlinear intrusion data to low-dimensional space, establishes the relationship mapping between high-dimensional and low-dimensional, and then uses fine-tuning algorithm to transform the model to achieve the best expression of features. At the same time, this method improves the data processing and method model without destroying the learned knowledge of the model and seriously affecting the real-time performance of detection. In order to overcome the problem of system instability caused by fixed empirical learning rate, this paper proposes a learning rate optimization strategy based on energy change. In the process of feature extraction, the features of different hidden layers are extracted to form combined features. Experiments show that the detection

Journal of Cyber Security and Mobility, Vol. 13_1, 1–26.
doi: 10.13052/jcsm2245-1439.1311

rate of this method can reach 95.31%, and the false alarm rate is 2.14%. This verifies the effectiveness of the secure computer database updating algorithm in this paper. Which can ensure the online update of the secure computer database.

Keywords: DBN, security computer, update database.

Introduction

With the development of economy and the improvement of information technology, all walks of life rely more and more on computer systems. Computer systems are not only widely used in all service industries such as data calculation, banks, schools, restaurants, etc., but also in cutting-edge science and technology industries such as electric power, military affairs and aerospace [1]. By improving efficiency as well as extending the marketplaces for products or activities, technologies can have an impact on growth. For instance, advances in modern farming have boosted acreage returns as well as improved nutrition stability. Because of its openness and complexity, the network has great security risks [2]. As the frequency of network users and network resources is increasing year by year, more and more major network security incidents frequently occur, which have a serious impact on people's lives. At the same time, some industries have very high requirements for the safety and reliability of computer systems, and the safe and reliable operation has a great impact on people's lives and property. Therefore, it is necessary to take very effective measures to continuously improve and perfect the update mechanism of secure computer database [3]. As far as the new-type secure computer in the current era is concerned, it not only needs to have a good hardware foundation, but also needs to meet the application update requirements of the database. Therefore, there are many factors to consider in the updating mechanism, which should be adjusted according to the actual demand [4]. Security situation refers to the current security state and changing trend of the whole environment, which is composed of security demand factors such as the real-time running status of computing equipment, service mode, service content and tenant behavior. Situation prediction is to do real-time security analysis in the computing environment, and capture the factors that can cause the security situation to change. Adopting fault-tolerant system can improve the reliability and security of the system [5, 6]. Fault-tolerant system refers to the technology that can still ensure the overall running security of the system when one or more components of the system

have errors. Nowadays, fault-tolerant systems are increasingly used in key fields such as aircraft control systems and industrial controllers. Because the application function of the new security computer database update mechanism is comprehensive, it must have a good guarantee on the basic hardware conditions [7]. Enhance safety by encryption the backups on that location in as well as keeping it somewhere. The information is safe when you use a secondary data model, although if the central server is corrupted or unavailable. In the past, the efficiency of ordinary data processing was very high. There are three basic types of information handling: physical, electrical, as well as organic. However, when updating the information of complex databases, this way of updating each system independently can't comprehensively update and vote on multiple databases in time, so it is necessary to find a faster updating way.

The birth of deep learning has brought a new breakthrough to the expression of machine learning features. It has excellent feature learning ability by constructing artificial neural network with more hidden layers; Moreover, it has a great advantage over other models through unsupervised learning of "initialization step by step" when training models [8]. There are three mature frameworks for deep learning, namely DBN, sparse self-coding machine and convolutional neural network [9]. A deep belief network (DBN) is a type of deep learning prototype used in computer vision. It is made up of numerous levels of factor loadings, or hidden nodes, with interconnections among the levels but not among the components in every level. DBN is a stack of several RBM (Restricted Boltzmann Machine), and RBM is trained layer by layer from bottom to top when training the network. RBM network includes a two-layer network structure model of visible layer and hidden layer [10]. A generating probabilistic convolutional neural network that could acquire a posterior distribution across its number of parameters is considered a limited Boltzmann model (RBM). Constrained Boltzmann Computers are probabilistic two-layered neuronal systems that can dynamically identify underlying structures in information through recreating data. They are a subset of energy-based systems. They contain two levels, one of which is concealed. According to the practical application, the visible layer is also called the data input layer, and the hidden layer can be called the feature extraction layer, and the nodes of the two layers are connected by weight parameters. In this network, the RBM of each layer is trained separately [11]. RBM can be regarded as an undirected graph model, which has a visible layer and a hidden layer. The layers are all connected, but there is no connection within the layers. Through its multi-layer nonlinear transformation, it trains deep abstract features from

complex cloud security situation data to describe the internal relationship of data [12]. Based on DBN technology, this paper proposes a secure computer database updating algorithm. Its innovations are as follows:

(1) In this paper, the model adopts multi-layer depth structure for unsupervised feature learning, maps high-dimensional and nonlinear intrusion data to low-dimensional space, establishes the relationship mapping between high-dimensional and low-dimensional, and then uses fine-tuning algorithm to transform the model to achieve the best expression of features. In the process of feature extraction, the features of different hidden layers are extracted to form combined features. In addition, the algorithm in this paper does not directly vote on the database, but votes on the state of the database to solve the problem of excessive voting data. At the same time, the database versions among multiple lines can be compared in real time.
(2) In this paper, the data processing and method model are improved without destroying the learned knowledge of the model and seriously affecting the real-time performance of detection. At the same time, in order to overcome the problem of system instability caused by fixed empirical learning rate, this paper proposes a learning rate optimization strategy based on energy change.

Based on DBN, this paper analyzes the update algorithm of secure computer database. The full text is divided into five sections. The following is an overview of each section:

The first section is introduction. This section mainly introduces the background of this topic, the purpose and significance of the research. The second section summarizes the related research literature and the research methods of this paper. The third section is the method part. Firstly, this section makes a simple analysis and introduction of the hardware technical framework of the security computer system. Then it introduces the concept of deep learning, the theory of DBN and its training methods. Finally, based on DBN technology, a secure computer database updating algorithm is proposed. The fourth section tests and analyzes the algorithm.

Related Work

Hiraoka et al. established a comprehensive situation assessment index system, which laid a foundation for improving the accuracy of cloud security situation prediction [13]. Gao et al. pointed out that when the security computer is

updating the database, because the data volume of the database is very large, the security computer cannot directly vote on the database data [14]. In this case, other methods must be taken to ensure the security of the system when the database is updated. Based on the status quo of the update mechanism of secure computer databases, Theodoridis et al. studied their algorithm by using the method of updating the data status in the database rather than the information in the database [15]. Hazrati et al. constructed sample data for cloud security situation prediction, and realized the mapping between situational elements and predicted values through DBN; and combined with the improved DE (Differential Evolution) to optimize the network parameters of the hidden layer [16]. Finally, the simulation results show that the prediction accuracy is improved compared to the existing cloud security situation prediction models. Park et al. applied multiple comparative experimental datasets to the DBN model respectively, obtained a data optimization processing method that could improve the detection results of the DBN model, and used the model to detect unknown types of attacks [17]. Kudo et al. introduced the hardware architecture of a three-out-of-two secure computer; then analyzed the requirements for the database update function based on the hardware architecture, as well as the general design and detailed design of the software modules; and introduced the database update method. The protocol that needs to be used [18]. Pucciani et al. proposed an algorithm for updating the secure computer database and possible problems, which improved the update rate of the secure computer database and the safety and reliability of the computer's long-distance travel [19]. Marcozzi et al. proposed a DBN-based hybrid intrusion detection model. In this model, a DBN with a 5-layer structure is used as the feature learning process, and then a support vector machine is used to identify and classify intrusions [20]. Both signature-based intruder identification as well as anomaly-based invasion monitoring are widely used by detection techniques. Through the use of network activity as well as user data, signature-based access control can identify risks by correlating them to established detecting attacks. Stosovic et al. have high adaptive ability for intrusion detection requirements. The sampling of the contrastive divergence algorithm in traditional DBN is easy to fall into the local optimal value and the learning rate parameter is sensitive in the training process. In several machine learning techniques, including limited Boltzmann machines as well as fully connected networks, the meta-discourse convergence technique is a common method for developing energy-based latent factor concepts. Assuming a probability density function more than a matrix, in which is a hiding factor, is an efficiency functional, & is a normalization

factor or partitioning feature. There are several fields where this type of probability sampling has been applied. An intrusion detection algorithm based on adaptive DBN is proposed [21]. Muralidhar et al. used Markov's model to model and compute the proposed database update mechanism [22–24]. The calculation results show that the database update mechanism can fully meet the requirements of security and reliability.

At present, in the operation and management of secure computer database, although the basic management technology has reached a certain level, there are obvious problems in the update mechanism of secure computer database. Especially in the lack of basic information interaction, which affects the later use. Based on this, this paper mainly studies the update mechanism of secure computer database. Based on DBN technology, this paper proposes a secure computer database updating algorithm.

Methodology

Related Theoretical and Technical Basis

At present, the new security computers used are generally two out of three computers. This computer often includes three units, namely ATP (Automatic Train Protection), ATO (Automatic Train Operation) and COMM (Communication Board). A sort of train security technology termed automatic train prevention (ATP) constantly verifies that a vehicle's velocity is consistent with the authorised velocity permissible through communication, incorporating automated stopping at specific signaling features. In the event that it isn't, ATP engages a hand brake to halt the locomotive. Technologies entitled automatic speed operating (ATO) is utilized to manage railway operating. ATO is mainly utilized on automatic guardrail transport as well as speedy transport networks because these technologies make it simpler to assure safe operation. A youngster will acquire to gesture at a template of characters, drawings, or photographs on an information board in ability to talk with others. These three units cooperate with each other and are responsible for different work contents. Two-out-of-three security computer consists of three systems, each of which has an ATP unit, and the three ATP units among the three systems are connected by point-to-point Ethernet [25–28]. There is an ATO unit in the first and second series of three series, but there is no ATO unit in the third series. There are three COMM units in the two-out-of-three security computer system, and each COMM unit is connected to all three systems point by point. The general component of the two-out-of-three

structure is three computer systems, which do not interfere with each other during operation. Then, through debugging, they can run at the same time, and the required time and speed are consistent. When the three systems generate corresponding data information after each cycle operation, the final data result can be produced by two-thirds voting. Two-out-of-three security computer is composed of three computer systems that run independently. The three computer systems synchronize their cycles, and each system outputs data every cycle. The data of three systems becomes the final output result after two-out-of-three voting. Security computer software is divided into platform software and business software. Software concept considered encapsulating limits accessibility to information and operations within an entity, restricting its usage or modification by outside resources. Systems that are object-oriented, like Java, frequently use confinement. The information may be shielded against immediate accessibility as well as manipulation that could result in errors. Platform software is the core of security computer software, which is responsible for encapsulating things at the hardware level. Information as well as systems currently vary most noticeably in that program is a stand-alone commodity that may interface with some other programs or systems, whereas operating systems host programs and supply capabilities. It includes periodic synchronization of the three systems, voting on the input and output of the three systems, communication with external data and various details of internal data transmission. Whenever a mobile phone interacts with software running on a desktop or a server, synchronization takes place. Common terms for this include synchron or landing. The CPU retrieves as well as performs the basic requirements. in order, one by one, from storage where they are cached. In reality, this list of instructions constitutes the very basic software program. In order to improve the effectiveness of the database update mechanism, the new security computer also needs to have three departments, and ATP units need to be closely distributed in each department, and the connection between each department is mainly accomplished through Ethernet. Security mechanisms are divided into three main categories. These encompass physical safety measures as well as managerial safety and operating safety precautions. Inform the workforce that keeping the network safe serves not just the needs of the company but additionally the requirements of the customers. Educate employees about safety concerns. Make sure your personnel have the necessary security education. Watch user behaviour to evaluate the cybersecurity strategy. In order to safeguard confidential material from getting into the incorrect hands, operational security (OPSEC), often referred to as procedures safety, is a portfolio management method that

motivates executives to look at activities from the viewpoint of an enemy. Physical security is the safeguarding of people, equipment, systems, and information against actual aggression and occurrences that might seriously harm a business, government entity, or organization. When the two-out-of-three structure is applied to general small-scale data, the data will be voted in turn, and the accuracy is particularly high, so it can achieve good application results. However, in the face of complicated and large-scale databases, the disadvantages of the two-out-of-three structure are undoubtedly exposed. A data structure guarantees data safety as well as confidentiality by trying to ensure that only authorized users have connection to the information and by performing permission procedures if unauthorized to critical material is requested. The phrase big information analytics refers to a broad category of methods and technologies used to analyse large amounts of information. It is often carried out using either MapReduce-powered platforms or concurrent database management platforms (DBMS). Due to its simplicity, structural DBMS is the greatest popular DBMS paradigm. The foundation of this approach is the normalization of the information in the server's rows or columns. Database paradigm that is maintained in set hierarchies but is controlled via SQL.

Deep learning is an algorithm that attempts to abstract data through a series of multi-layer nonlinear transformations. It can use many simple neurons to construct multilayer neural networks. Among the existing deep learning models, the deep learning method based on DBN is in the leading position. In order to address the issues with typical neural systems retraining in deeply layered networking, including slow development, obtaining trapped in global minimum owing to poor optimization method, and needing a large amount of working information, deep belief systems (DBNs) was developed. DBN can be utilized to complete controlled academic goals to create categorization or prediction algorithms as well as unstructured learning opportunities to lower the complexity of subspace. Mainly because it takes the restricted Boltzmann machine as the network infrastructure, and can be stacked layer by layer to form a multi-layer structure. There is a nonlinear mapping relationship between input and output. Multi-layer abstract feature expression is formed in the process of automatic and unattended learning from bottom to top. As we delve further into the system, there are more limitations. Because we pooling, the geographical dimension of the feature mappings shrinks, but as we add additional filtering, the complexity of the regions grows. According to the network structure formed in the learning process, the system maps the input training sample data into the network

features at all levels, and then uses the classifier or matching algorithm to complete the top-level output process, and finally completes the prediction or classification of the samples. RBM model structure can be described as a directed acyclic graph. RBM is a component of DBN, so DBN is a directed acyclic graph with high complexity. Unsecured activity involving includes creating an uncontrolled fully convolutional network utilizing the aggressive layer-wise method, where a recognized network output is recently expanded. In some applications, RBM can also be used as an independent model method to solve the problems of feature extraction, classification and clustering. RBM pre-trains by unsupervised greedy way to get the weights of the generated model. DBN can be divided into two steps in the process of training the model: (1) Pre-training. A layer-by-layer pre-training process, through an unsupervised greedy layer-by-layer method to pre-train to obtain the weights of the generated model. (2) Fine tuning. After the first pre-training, the network uses the labeled data to fine-tune the weights of the network by algorithm. The network structure is shown in Figure 1.

Due to the multiplicity of connections, different hardware facilities often have redundant relationships. Dynamic redundancy, in which additional elements are engaged upon the breakdown of an active ingredient, is a specific variety of physical duplication. Composite equipment redundancies, which

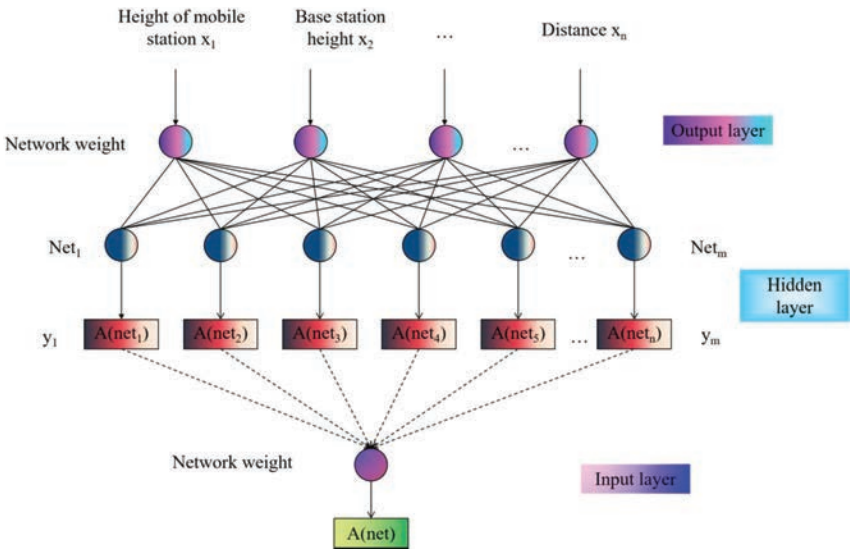


Figure 1 Network structure diagram.

combines stable as well as active reliability approaches, is another option. That is, if one COMM unit in this security computer keeps working, the other one will automatically enter the standby state, so that it can be used in time when there is a problem in the working unit, and it is not easy to be interrupted. The form of company as well as entire workplace atmosphere play a role in identifying the greatest prevalent workplace problems, but in principle, areas of concern can be divided into four main groups: interaction, harassing as well as intimidation, gossiping, or enhance team. When voting on large-scale data information, the best way is to change it into some content with small capacity and vote quickly and effectively. The operation of business software on CPU is based on database data. When the system detects that the database version is old, the business software will request database update. When the status of the database becomes updatable, the platform software transports the database to the protected memory through the bus, and sets the database update status in the shared memory as update complete. Voting is a process that a gathering, like an assembly or gathering, can use to reach a consensus or form an opinion, typically after talks, arguments, or electoral politics. Although when national or local elections are conducted with roughly identical contenders, topics, as well as timings, each person's ranking of the significance of various criteria, such as allegiance, happiness, profession, ethnicity, race, and wealth, could be significantly distinct. In the operation of the new security computer database update mechanism, the voting mode of the database is very critical, which will also affect the information processing and application of the database. If the available database content is very small, the occupied bytes will be relatively small. The efficiency of the model may be impacted by the quantity of a material collection. Generally speaking, companies shouldn't let information warehouses go bigger than 200 GB. At this time, the data packet can fully reflect the overall situation of the database, and the voting on the secure computer database can be completed. At present, the security computer can't directly vote on the track database or other large-scale data. By setting up login credentials and using the DBMS to manage authentication procedures, accessibility regulation is achieved. As a result, accessing to critical data stores is limited to network customers who have permission to do so, and it is not available to anyone else. Generally, the large-scale data is only updated by a single system, and the security of the data is ensured by means of verification. Therefore, a secure computer database update mechanism based on state voting came into being. According to the structure, the state of database update of security computer based on state voting can be divided

into three components: capacity, model and state, which are the basis of database update voting.

Design of Update Mechanism of Secure Computer Database

The adaptive DBN algorithm is based on the change of RBM energy, and takes advantage of the fact that the minimum RBM energy is the most stable state of the system. A novel supervised learning algorithm is proposed, which can make the sampling of the algorithm global and the stability of the algorithm strong. It is the level-by-level expression of DBN structure that makes it possible to refine and screen intrusion data through this level-by-level expression depth structure when dealing with a large number of intrusion detection data, which brings great help to the detection performance of intrusion detection system. In the new security computer database update mechanism, the update status of the database has multiple links with its own status, but in general, it is normal output, and the corresponding database update is relatively stable. Sometimes the output is normal, but the update is abnormal. Whenever conduct is unusual or outside the standard, includes unwanted behaviour, and impairs a person's performance, it is deemed irregular. Conduct that is deemed unusual is anything that differs from sure the organization, economic, as well as economic norms. Upgrades repair any software or equipment issues that weren't discovered prior the item was made available to the general public. If you do not even upgrade, the machine may have these issues or be exposed to threats. When the security computer database is updated, other programs cannot be run. You must wait for the update to be completed before proceeding with other programs. If there is a problem in one of the systems, you can switch to other modes to keep the other two systems running. In this paper, the corresponding labeled neurons of each group of training data are turned on and set to 1, while the rest are turned off and set to 0.

Assuming that each node takes values between sets $\{0, 1\}$, that is:

$$\forall i, j, v_i \in \{0, 1\}, h_j \in \{0, 1\} \tag{1}$$

The state of the ith visible layer node is v_i; the jth hidden layer node state is h_j; the calculation method of the (v, h) RBM energy function for the network state is as follows:

$$E(v, h|\theta) = -\sum_{i=1}^{n} a_i v_i - \sum_{j=1}^{m} b_j h_j - \sum_{i=1}^{n} \sum_{j=1}^{m} v_i W_{ij} h_j \tag{2}$$

Among them, $E(W_{ij}, a_i, b_j)$ is the RBM parameter; W_{ij} is the connection weight between the visible node i and the hidden node j; a_i is the bias of the visible node i; b_j is the bias of the hidden node j. When the parameters are determined, the energy function can obtain the joint probability distribution of (v, h):

$$P(v, h|\theta) = \frac{e^{-E(v,h)}}{Z(\theta)}, Z(\theta) = \sum_{v,h} e^{-E(v,h|\theta)} \tag{3}$$

Among them, A$Z(\theta)$ is the normalization factor. A procedure that increases normality or regularity is referred to as normalizing or legitimization. Usually frequently, it alludes to normalization (social sciences), also referred to as normalization, that is the procedure whereby concepts and actions that may defy accepted social standards are viewed as normal. It gives back a number among 0 and 1. Two issues with nonlinear activation algorithms stand out: Differences of exponential exhaust as well as destroy for a high affirmative or huge negatives integer, the outcome of a logistic permeates (i.e., the slope goes parallel towards the x-axis). The activation probability of the jth hidden unit is:

$$P(h_j = 1|v, \theta) = \sigma\left(b_j + \sum_i v_i W_{ij}\right) \tag{4}$$

Among them, $\sigma(x) = \frac{1}{1+\exp(-x)}$ is the activation function of Sigmoid.

In artificial neural systems, an activating functional is a variable that produces a lower size for tiny values as well as a higher price if its contributions are greater than a barrier. The activating functional fires if the supplies are big sufficient; else, everything happens. If the relevant parameters of the network are not properly selected, the accuracy of the prediction results may be seriously reduced or the training time is too long. Because its focus is the collection of all actual figures as well as its extent is, the linear function is however characterized as a squashing functional (0, 1). To solve these problems, the core idea of DE is integrated into DBN to simplify the network structure and build a deep learning model with good performance. The mathematical description of DE algorithm is shown in the formula:

$$DE = \{g_0, m_0, l_0, q_0, f_0, b_0, c_0\} \tag{5}$$

Among them, g_0 is the number of nodes in the hidden layer of the DBN network; m_0 is the parameter of the hidden layer of the DBN; l_0 is the

population size; q_0 is the fitness function of the individual. And define three operations: f_0 is a copy operation; b_0 is a crossover operation; c_0 is a mutation operation.

Taking three out of two security computers as an example, when the three systems output the same database state, there are C_3^1 combinations; when the three systems output two different database states, there are $C_3^2 C_2^1$ combinations; when the three systems output three different databases There are C_3^3 combinations in the state. The number of combinations of three-series output database states is as follows:

$$sum = C_3^1 + C_3^2 C_2^1 + C_3^3 \tag{6}$$

Assumed initial conditions:

$$P_0(0) + P_1(0) = 1, P_S(0) = 0, P_F(0) = 0 \tag{7}$$

That is, the system starts to be in a normal two-out-of-three or two-out-of-two working state, and after Laplace transformation, the following results are obtained:

$$P_0(t) + P_1(t) = e^{-(i+k+m)t} \tag{8}$$

$$P_S(t) = \frac{i(j+n-i-k-m)+jm}{(j+n-i-k)(j+k+m)}[1 - e^{-(i+k+m)t}] \tag{9}$$

$$P_F(t) = \frac{k(j+n-i-k-m)+mn}{(j+n-i-k)(j+k+m)}[1 - e^{-(i+k+m)t}] \tag{10}$$

The reliability of the system is:

$$R(t) = P_0(t) + P_1(t) \tag{11}$$

The security of this system is:

$$S(t) = P_0(t) + P_1(t) + P_S(t) \tag{12}$$

When the system is in an orderly state or the probability distribution is more concentrated, the system energy will be smaller; However, when the system state is disordered or the probability distribution tends to be uniform, the system energy will increase. Therefore, the system can reach a stable state after many state transitions, and the minimum value of the energy function corresponds to the most stable state of the system.

SRTP (Secure Real-Time Transport Protocol) protocol is designed for data transmission in the secure computer platform. The Security Real-time Transportation System (SRTP) is a Real-time Transmission Platform (RTP) feature created to safeguard RTP information against various attacks as well as to offer communication cryptography, identification, as well as authenticity. By encryption the RTP content but not the RTP preamble, SRTP protects the data. It is frequently utilised as the network security for RTP as well as offers resource location verification. It is important to apply it entirely, but you can either deactivate or activate some critical factors. A security model entitled SRTP adds a number of cryptographic methods towards the Real-time Transmission Standard (RTP). Speech across IP (VoIP) as well as graphic transmission or broadcasting employ SRTP, a secured variant of the Real-Time Transportation Protocols. The connection in the secure computer platform involves serial port, CAN and Ethernet, and the database update only involves the Ethernet part of SRTP protocol. The list of SRTP messages is shown in Table 1.

The interaction diagram of SRTP timing synchronization is shown in Figure 2.

For the analysis of different situations, it is necessary to improve the scientificity of the voting algorithm. The existing conditions are used to analyze the database update, so as to ensure that the voting algorithm can meet the needs of database update, thus ensuring the stable update of the database. Usually, information gain is used to evaluate the amount of information that attributes can reflect in the process of intrusion judgment. If the information gain value of a certain feature attribute is larger, its proportion in the process of intrusion identification will be more obvious. Therefore, when selecting data features, this paper chooses information gain method to select feature

Table 1 List of SRTP messages

Name	Name Specification
CSD	Secure data message, a message used for secure data transmission
CSE	Timing request message, which is matched with CSR message and used for timing synchronization
CSR	Synchronous response message
KAD	Keep Alive message, used to maintain the connection status
CIE	Initialization request message, used to establish connection request
CEE	End of connection request message, used to disconnect
ACK	Reply message
NAK	Non-response message

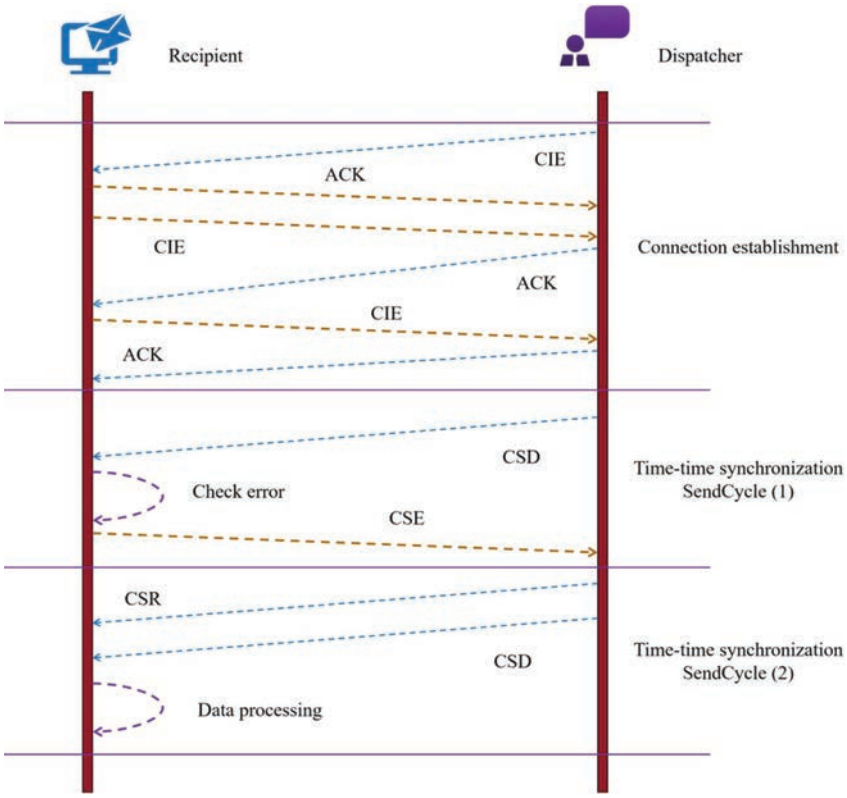


Figure 2 SRTP timing synchronization interaction diagram.

attributes as the basis of intrusion feature selection. Acquire, analyze and preprocess data sets. In this paper, different data preprocessing methods are used to process the same data set, so as to form a number of different data sets, in order to choose the best data processing method for DBN algorithm, and at the same time verify the influence of data processing methods on classification results. Contrast divergence algorithm is a very important RBM training algorithm and learning method of deep neural network, which can improve the training speed of the algorithm.

Result Analysis and Discussion

In this paper, the DBN network model with good learning ability is selected to solve the problem of updating the secure computer database.

The experimental environment is: Windows operating system; MATLAB software. The computer hardware platform adopts MPC processor, and the COMM board is the external communication board. The three systems are interconnected by point-to-point Ethernet. COMM board is connected to each system point by point through Ethernet, and two comms are redundant with each other. For each department, two COMM boards constitute the external communication platform of the department. In this paper, NSL-KDD data set is used to evaluate the algorithm. It solves some problems inherent in KDD 99 data set. The NSL-KDD training dataset is an update to the KDD'99 time series. Investigators can use this benchmarking set of statistics to evaluate various intrusion prevention strategies effectively. A standardized collection of auditable information, including a wide range of simulated assaults into a government distributed system, is contained in this dataset. The KDD-99 information set's precursor, the NSL-KDD set of data points, has been improved. The NSL-KDD training dataset is examined as well as employed in this study to investigate how well different classification methods can identify abnormalities in system traffic. Such as redundant records in the training set, so the classifier will not favor more frequent records; Moreover, the number of records in the training set and the test set is reasonable, so that the data set can be fully utilized in the safety detection test. In the training data and test data, some duplicate data are removed, so that each attack has only one record in the data set. Data redundancy is a method used in computers to get rid of extra versions of repeated content. Every stretched practice needs to be done for a minimum of 60 secs for best effects. Therefore, it'd be excellent to perform a stretching three more times if you're able to maintain it for 15 seconds. It should be sufficient to perform two additional rounds if you're able to sustain the stretching for 20 seconds. Firstly, NSL-KDD digitizes the character data in the data set, and then normalizes the data. Among the features of safety detection data sets, some of them not only have no positive influence on the recognition effect of abnormal data, but may interfere with the distribution of data due to the existence of these features, thus reducing the classification accuracy of data by the model. In the data preprocessing stage, the algorithm in this paper processes different types of data respectively. The normalization of data is to eliminate the differences of different attributes and avoid the influence of measurement units on the evaluation results of the algorithm. There are more alternatives besides the min-max normalisation procedure. The underlying data acquired will be modified in the 0 to 1 domain by using min-max normalisation (inclusive). The reason why normalisation must be carried out can be briefly explained

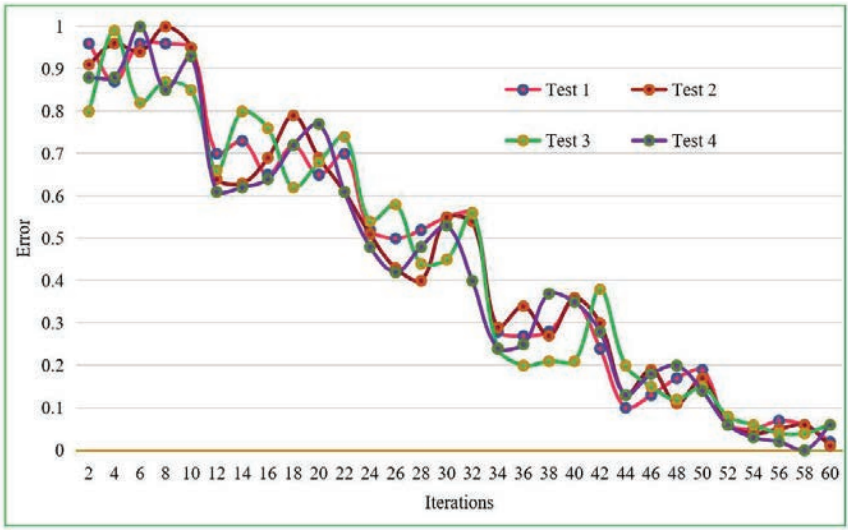


Figure 3 Training results of the algorithm.

in terms of perceptron. In order to process data conveniently and improve the convergence speed of the algorithm, this paper will map the intrusion detection data to the range of 0∼1 by using the method of min-max data normalization. The training results of the algorithm are shown in Figure 3.

In the model design stage of DBN, the final network structure with the highest recognition rate for unknown types of attacks is determined by controlling other parameters unchanged, changing one parameter for repeated verification and cross-verification. In order to determine the choice of parameters, this section will repeat the experiment with different parameters. First, determine the number of RBM iterations. Secondly, determine the number of hidden layers. Finally, the number of hidden layer nodes is determined. In this paper, we have done a lot of repeated experiments when adjusting these parameters. Table 2 shows the influence of different iterations on the results. Table 3 shows the influence of the number of different hidden layers on the results. Table 4 shows the influence of the number of hidden layer nodes on the results.

The data selected from different groups of original data is inversely proportional to the size of the original data, which makes the classification types obtained by machine learning method more diverse, and can effectively evaluate the performance of different algorithms. And that curve of safety and reliability are shown in Figure 4.

Table 2 Influence of different iteration times on the results

Iterations	1	5	20	100
Number of hidden layers	4	4	4	4
Number of hidden layer nodes	80, 60	80, 60	80, 60	80, 60
Error rate	0.1631	0.1486	0.1836	0.2187

Table 3 Influence of the number of different hidden layers on the results

Iterations	4	4	4	4
Number of hidden layers	1	2	3	4
Number of hidden layer nodes	80	80, 60	80, 80, 60	80, 80, 80, 60
Error rate	0.1564	0.1421	0.1237	0.1601

Table 4 The influence of the number of hidden layer nodes on the results

Iterations	4	4	4	4
Number of hidden layers	4	4	4	4
Number of hidden layer nodes	80, 60, 60	60, 60, 80	80, 60, 50	220,160,60
Error rate	0.1531	0.1521	0.1386	0.2639

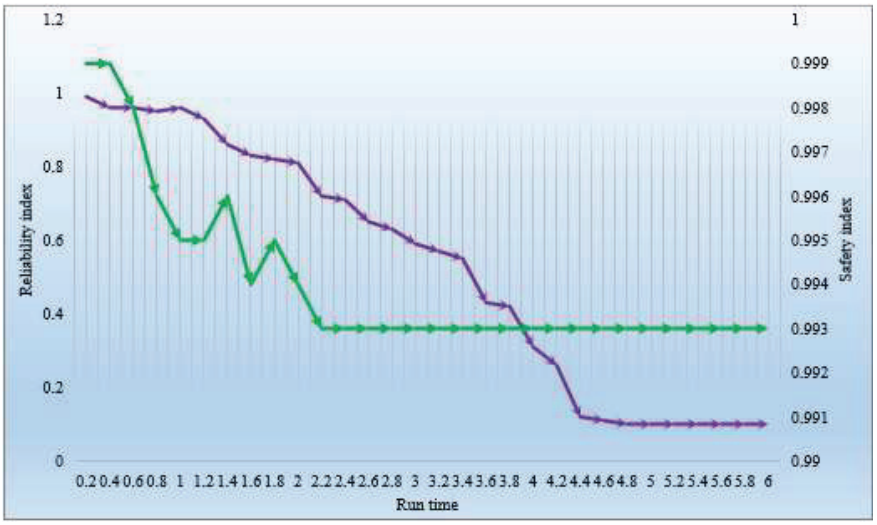


Figure 4 Safety and reliability graph.

It can be seen that both of them decrease with time, and the security is infinitely close to 0.9 with time. With the increase of time, the reliability is infinitely close to 0. Because the errors in the database are random, the results of different erroneous data calculations are different. When voting, the data

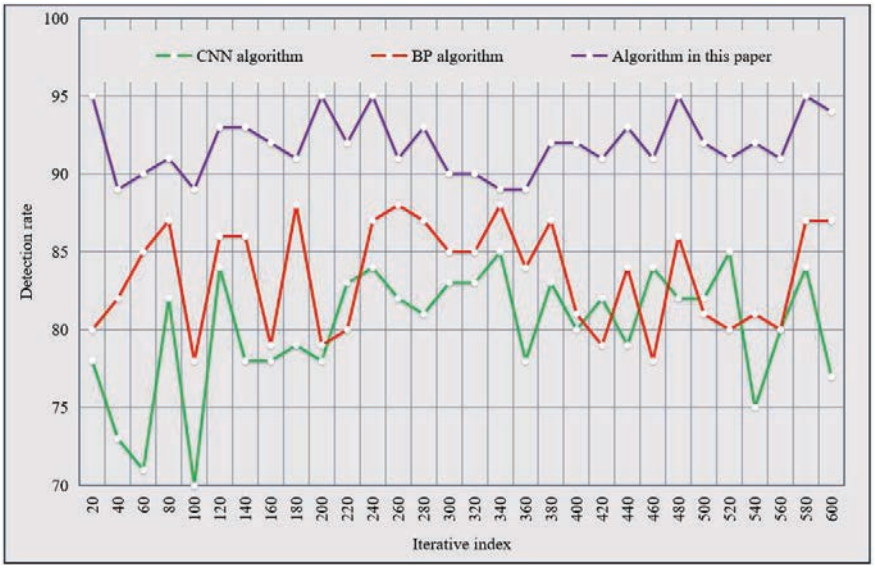


Figure 5 Detection rate results of different algorithms.

of three series are different in the two-out-of-three mode or the data of two series are different in the two-out-of-two mode, which will cause this data to be discarded. At this time, the voting module will give an alarm, and if there is no data output for three consecutive cycles, the system will restart.

The feature dimension of the test data is consistent with the dimension of the training data, and it is input into the DBN network to get the classification result of the test data. Because the classification label of the test data set is known, by comparing the classification result output by the selected DBN network with the known data classification label, we can get the correct detection rate and real-time performance of the model for the test data. The detection rate results of different algorithms are shown in Figure 5. The degree of all disruptions, such as sound, congestion, or jammer, affects the false alarm rate. The impact of the permanent congestion is greater than the degree of disturbance close to the radar location. The impact of sound levels is greater at a range. The result is that the rate of false alarms is range-dependent. Improper or misinterpreted numeric priority, Multipathing procedures, Wrong startup, Wrong granularity consistency, and Wrong graphical expression of an argument. The false alarm rate results of different algorithms are shown in Figure 6. The detection time-consuming results of different algorithms are shown in Figure 7.

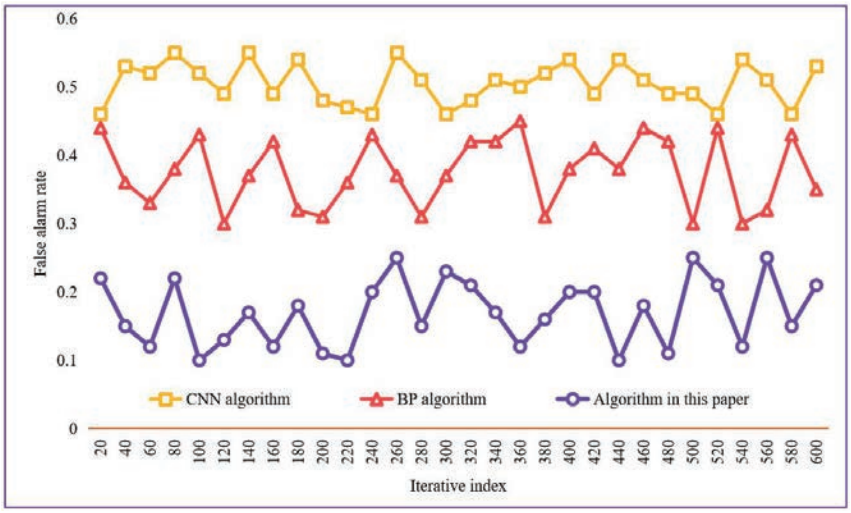


Figure 6 False alarm rate results of different algorithms.

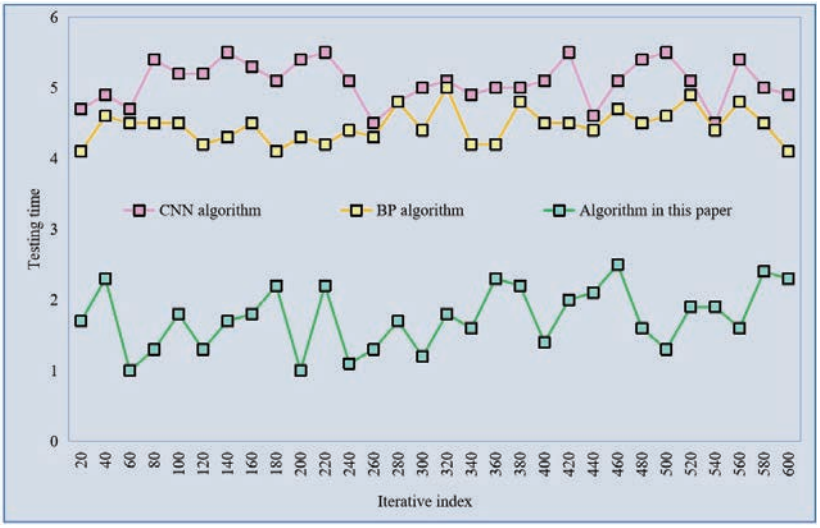


Figure 7 Detection time results of different algorithms.

By adding test code on the basis of source code to simulate all kinds of update errors, the test code simulates all kinds of update errors. As long as the database is updated, the test code will automatically inject faults. Experiments show that the detection rate of this method can reach 95.31%,

and the false alarm rate is 2.14%. This verifies the effectiveness of the secure computer database updating algorithm in this paper.

Conclusions

At present, it is very important to update the computer database. However, there are quite a few shortcomings in the current computer database, and the updates are prone to management and data missing errors, which will easily bring various influences to the later application. In order to ensure the security of large-scale data transmission in a short time and in a wide range during online database updating, this paper presents a secure computer database updating algorithm based on DBN. In the process of feature extraction, the features of different hidden layers are extracted to form combined features. In addition, the algorithm in this paper does not directly vote on the database, but votes on the state of the database to solve the problem of excessive voting data. At the same time, the database versions among multiple lines can be compared in real time. Methods On the basis of not destroying the learned knowledge of the model and not seriously affecting the real-time performance of detection, the data processing and method model were improved respectively. At the same time, in order to overcome the problem of system instability caused by fixed empirical learning rate, this paper proposes a learning rate optimization strategy based on energy change. Experiments show that the detection rate of this method can reach 95.31%, and the false alarm rate is 2.14%. This verifies the effectiveness of the secure computer database updating algorithm in this paper. This method is very suitable for data extraction in high-dimensional space, which greatly reduces the time complexity of security detection training. It is a feasible and efficient algorithm for updating security computer database. This research provides a new direction for the update of computer database, in order to promote the stable development of the update mechanism of secure computer database. How to detect emerging new network attacks and how to apply DBN theory to automatic feature extraction of abnormal worms is an important research direction in the future.

Data Availability

The figures and tables used to support the findings of this study are included in the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Funding Statement

The authors would like to thank the financial supports from Henan Province Philosophy and Social Sciences "Research on the Coin Database of central plains" (Grant No: 2021BLS002).

Acknowledgements

The authors would like to show sincere thanks to those techniques who have contributed to this research.

References

[1] Qiang W, Fz A, Jian X A. Efficient verifiable databases with additional insertion and deletion operations in cloud computing[J]. Future Generation Computer Systems, 2021, 115:553–567.
[2] Bella G, Curzon P, Lenzini G. Service Security and Privacy as a Socio-Technical Problem: Literature review, analysis methodology and challenge domains[J]. Journal of computer security, 2015, 23(5):563–585.
[3] Shakhovska N, Boyko N, Zasoba Y. Big Data Processing Technologies in Distributed Information Systems[J]. Procedia Computer Science, 2019, 160(2):561–566.
[4] Lazouski A, Martinelli F, Mori P. Usage control in computer security: A survey[J]. Computer Science Review, 2010, 4(2):81–99.
[5] Denning T, Kohno T, Levy H M. Computer Security and the Modern Home[J]. Communications of the ACM, 2013, 56(1):94–103.
[6] Zhan S, Yu L, Wang Z, Du Y, Yu Y, Cao Q, Dang S, Khan Z. Cell traffic prediction based on convolutional neural network for software-defined ultra-dense visible light communication networks[J]. Security and Communication Networks. 2021, 19;2021.
[7] Feng D, Yajie M, Fengxing Z. A Safety Message Broadcast Strategy in Hybrid Vehicular Network Environment[J]. The Computer Journal, 2018, 61(6):789–797.
[8] Burr W, Ferraiolo H, Waltermire D. NIST and Computer Security[J]. It Professional, 2014, 16(2):31–37.

[9] Tseng F K, Liu Y H, Chen R J. Advances in Information and Computer Security[J]. Lecture Notes in Computer Science, 2013, 15(1):5–6.

[10] Maram B, Gnanasekar JM, Manogaran G, Balaanand M. Intelligent security algorithm for UNICODE data privacy and security in IOT[J]. Service Oriented Computing and Applications. 2019, 13(1):3–15.

[11] Igor H, Bohuslava J, Martin J. Application of Neural Networks in Computer Security[J]. Procedia Engineering, 2014, 69(15):1209–1215.

[12] Konur S. Specifying safety-critical systems with a decidable duration logic[J]. Science of Computer Programming, 2014, 80(10):264–287.

[13] Hiraoka Y, Murakami T, Yamamoto K. Method of Computer-Aided Fault Tree Analysis for High-Reliable and Safety Design[J]. IEEE Transactions on Reliability, 2016, 65(2):687–703.

[14] Gao Y, Gonzalez V A, Yiu T W. The effectiveness of traditional tools and computer-aided technologies for health and safety training in the construction sector: A systematic review[J]. Computers & Education, 2019, 138(SEP.):101–115.

[15] Theodoridis, Y. Ten Benchmark Database Queries for Location-based Services[J]. The Computer Journal, 2018, 46(6):713–725.

[16] Hazrati M K, Erfanian A. An online EEG-based brain-computer interface for controlling hand grasp using an adaptive probabilistic neural network.[J]. Medical Engineering & Physics, 2010, 32(7):730–739.

[17] Park S, Hong I, Park J. An Energy-Efficient Embedded Deep Neural Network Processor for High Speed Visual Attention in Mobile Vision Recognition SoC[J]. IEEE Journal of Solid-State Circuits, 2016, 51(10):2380–2388.

[18] Hou, Z. K., Cheng, H. L., Sun, S. W., Chen, J., Qi, D. Q., Liu, Z. B. (2019) Crack propagation and hydraulic fracturing in different lithologies. Applied Geophysics, 16(2), 243–251.

[19] Pucciani G, Domenici A, Donno F. A performance study on the synchronisation of heterogeneous Grid databases using CONStanza[J]. Future Generation Computer Systems, 2010, 26(6):820–834.

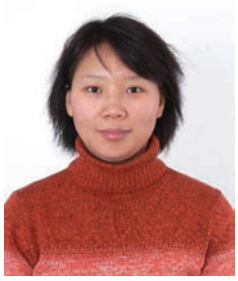
[20] Cheng, H., Wei, J., Cheng, Z. (2022). Study on sedimentary facies and reservoir characteristics of Paleogene sandstone in Yingmaili block, Tarim basin. Geofluids, 2022.

[21] Stosovic M A, Dimitrijevic M, Litovski V. Computer Security Vulnerability as Concerns the Electricity Distribution Grid[J]. Applied Artificial Intelligence, 2014, 28(4–6):323–336.

[22] Muralidhar K, Parsa R, Sarathy R. A General Additive Data Perturbation Method for Database Security[J]. Management Science, 2011, 45(10):1399–1415.
[23] Kudo T, Takeda Y, Ishino M. An Implementation of Concurrency Control between Batch Update and Online Entries[J]. Procedia Computer Science, 2014, 35(2):1625–1634.
[24] Han, J., Cheng, H., Shi, Y., Wang, L., Song, Y., Zhnag, W. (2016) Connectivity analysis and application of fracture cave carbonate reservoir in Tazhong. Science Technology and Engineering, 16(5), 147–152.
[25] Marcozzi M, Vanhoof W, Hainaut J L. Relational symbolic execution of SQL code for unit testing of database programs[J]. ence of Computer Programming, 2015, 105(Jul.1):44–72.
[26] BalaAnand M, Sivaparthipan C B. Security Privilege for Generating Session Key Using Selective Index for Passwords Validation[J]. Journal of Science and Innovative Engineering & Technology. 2013.
[27] Cheng, H., Ma, P., Dong, G., Zhang, S., Wei, J., Qin, Q. (2022). Characteristics of Carboniferous Volcanic Reservoirs in Beisantai Oilfield, Junggar Basin. Mathematical Problems in Engineering, 2022.
[28] Kundu A, Sural S, Majumdar A K. Database intrusion detection using sequence alignment[J]. International Journal of Information Security, 2010, 9(3):179–191.

Biographies

Liusuo Huang received his B.S degree in University of Information Engineering (Zhengzhou) in 1998. He is currently an associate professor in College of Software, Henan Finance University. His research interests focus on digital Humanities and database technology.



Yan Song received her M.S degree in Huazhong University of Science and Technology, 2016. Her is currently an associate professor in College of Software, Henan Finance University. Her current research field is software engineering and computer network technology.