Security Analysis of Car Driving Identification System Based on Deep Learning

Xiaogang Wei[1(✉)] and Rong Zhang[2]

[1] Chongqing Vocational Institute of Tourism, Chongqing 409000, China
xiaogang1987006@163.com
[2] Jiangmen Polytechnic, Jiangmen 529000, China

Abstract. The implementation of the car driving identification system will help to improve the safety and efficiency of navigation. The safety analysis technology can filter the attack events of the automatic identification system of car driving and reduce the error rate of safety analysis. To this end, a deep learning-based safety analysis method for car driving identification system is proposed. Based on the deep learning theory, a safety behavior analysis model of the car driving identification system is constructed. Through data collection, security analysis and response processing, the identification of abnormal communication security data strength is completed. A Cartesian coordinate system is established, and a heterogeneous data processing model is constructed. Based on the deep learning analysis process of security data, based on deep learning, by accessing system operation data, stream processing and data mining of security data, complete system security data defense control, and realize system security analysis. The experimental results show that the method in this paper has strong security analysis ability, and its matching range is large, which can match all security behaviors and reduce the error rate of security analysis.

Keywords: Deep Learning · Car Driving · Automatic Identification System · System Security · Security Analysis

1 Introduction

In recent years, the automatic identification system of car driving has been extended to the field of navigation, the confidential information in the automatic identification system of car driving has increased greatly, and the importance of the safety technology of automatic identification system of car driving has become increasingly prominent. How to effectively analyze the information and ensure the data security of the car driving identification system has become an urgent problem to be solved. As the number and severity of AIS attacks increases as the number of AIS users and information increases. Security analysis technology is an effective security method to discover a series of malicious behaviors that threaten the integrity, confidentiality and availability of information resources. For the large amount of event data of the car driving identification system, the

B. Wang et al. (Eds.): ICMTEL 2023, LNICST 532, pp. 468–484, 2024.
https://doi.org/10.1007/978-3-031-50571-3_34

safety analysis technology can accurately classify normal and abnormal events while considering the best classification rate. In order to achieve the purpose of filtering the attack events of the automatic identification system of car driving and reducing the false alarm rate [1].

At present, scholars in related fields have carried out research on system security analysis. Reference [2] proposes an aero-engine system safety analysis method based on the Simscape model. On the basis of the general characteristics of model-based safety analysis fault expansion, two ways of external fault expansion and internal fault expansion of modeling language in Simscape environment are analyzed to establish a coupled fault model. Taking the full authority digital engine control main fuel control subsystem as a research example, a formal system safety analysis of independent and coupled faults is carried out. This method ensures the consistency of design and safety analysis, but its safety analysis error rate is high. Reference [3] proposed an IMA system security analysis method based on AADL and HiP-HOPS. The AADL language is used to describe the system architecture and fault information, and the AADL architecture model is established. In order to further analyze its safety, the conversion of AADL model to HiP-HOPS model is proposed. Using HiP-HOPS, fault tree can be generated and IF-FMEA combined failure analysis can be performed, and safety reliability analysis of IMA flight planning system fault propagation can be carried out. This method can effectively reduce the error rate, but its security analysis ability is weak.

Aiming at the above problems, this paper proposes a safety analysis method for the automatic identification system of car driving based on deep learning. Establish a system safety behavior analysis model, and complete the communication anomaly safety data intensity identification through data collection, safety analysis and response processing. Build a heterogeneous data processing model, deeply learn and analyze the process based on security data, access system operation data, stream processing and data mining security data, complete system security data defense control, and realize system security analysis. The effectiveness of the method is verified by experiments.

2 Constructing the Analysis Model of the Safety Behavior of the Car Driving Identification System

Safe sex behavior analysis model is an important part of safety analysis technology. Based on deep learning theory, a deep learning classification model is established and simplified. This method has the characteristics of simplicity, high speed and high classification accuracy [4]. Its core algorithm is as follows:

Set the safety behavior as the sample $A = (a_1, a_2, \cdots, a_n)$, where the sample is a n dimensional Boolean vector. Divide the events of the car driving automatic recognition system into $C \in (C_1, C_2, \cdots, C_m, f)$, then there are m classification problems, where f is the mapping function. The training sample $X_1, X_2, \cdots, X_N$ is obtained according to the mapping function, where $X = (x_1\, x_2, \cdots, x_i)$, it can be seen that X is the t dimensional Boolean vector.

The calculation steps are:

(1) Calculate the probability of training sample c_j, expressed as $P(c_j)$, and the calculation formula is:

$$P(c_j) = \frac{\sum_{i=1}^{c} N_i(c_j)}{\sum_{j=1} T_j} \tag{1}$$

Among them, $N_i(c_j)$ represents the dataset of training samples c_j, and T_j represents the total sample dataset for training.

(2) Analyze the feature a_i in the training sample, and the relative probability value $P(a_i|c_j)$ of the feature value in the event category of the automatic identification system for car driving. The calculation formula is:

$$P(A = a_i|c_j) = \frac{\sum_{i,j-1} S(a_i \in \forall c_j)}{\sum_{j=1}^{c} N_j(c_j)} \tag{2}$$

Among them, $S(a_i \in \forall c_j)$ represents the sample set where the feature is located, and $N_j(c_j)$ represents the total number of feature samples.

(3) According to the above formula, the eigenvalues in the training samples are obtained, and the calculation formula is:

$$P(a_i) = \sum_{i=1,j-1}^{A \cup C} P(a_i|c_j)P(c_j) = \sum_{i=1,j-1}^{A \cup C} \frac{\sum_{i=1,j-1} S(a_i \in \forall c_j)}{\sum_{N} (c_j)} P(c_j) \tag{3}$$

(4) Use the deep learning automatic recognition system for car driving to obtain independent assumptions and analyze the probability of safe sexual behavior. The calculation formula is:

$$P(c_j|a_i) = \frac{P(c_j) \prod_{j=1} P(a_i|c_j)}{P(a_i)} \tag{4}$$

In order to obtain the topology structure of the directed acyclic automatic recognition system for car driving that can truly reflect the relationship between samples, the structure of the automatic recognition system for car driving is studied. The car driving automatic recognition system in this paper is able to display potential condition-independent relationships and probability distribution functions in the data.

According to the characteristics of the parameter learning method, the safety behavior analysis model of the car driving identification system can divide the parameter estimation into two categories: classical statistical estimation and deep learning statistical estimation. Two methods of moment estimation and maximum likelihood estimation are usually used for statistical parameter estimation. Maximum likelihood estimation is a common method in conditional probability table learning [5, 6].

Deep learning is divided into two stages, namely structural learning and parameter learning. Structural learning is to realize information analysis through the topology structure of the car driving identification system, and explore the conditional probability of learning the node variables inside the car driving identification system.

The deep learning car driving automatic recognition system can well train the sample data, and use the research to analyze the data and prior knowledge, so as to obtain the best car driving automatic recognition system topology. The reasoning methods of the deep learning car driving identification system include causal analysis, diagnostic analysis and support analysis to realize information reasoning. Causal reasoning adopts bottom-up reasoning. After analyzing the cause, a conclusion is drawn, and the reasoning that different phenomena appear under different circumstances is verified according to the known evidence. The diagnostic reasoning is different from the causal reasoning, which uses the conclusion to analyze the cause, and determines the probability of the cause after determining the reasoning result. Supporting reasoning is the analysis of data by verifying the interaction between different causes. The deep learning car driving automatic recognition system is used as the probability of car driving automatic recognition system. Through statistical research on knowledge classification, in a large database, different attribute values are judged and the accuracy of the method is improved.

The workflow of the safety behavior analysis model of the car driving identification system based on deep learning is shown in Fig. 1.

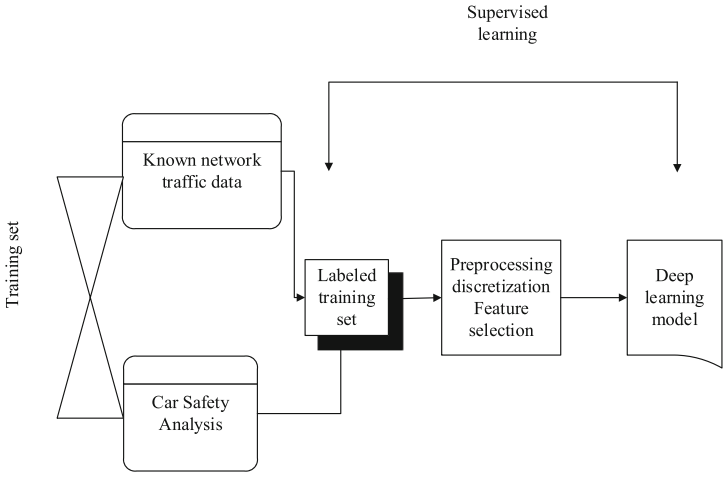


Fig. 1. Workflow of the system safety behavior analysis model

It can be seen from Fig. 1 that in the first stage, the flow data of the automatic identification system for car driving is analyzed. After different analysis types are identified, the mapping set is obtained as $U_{TC} = (T_k, C_k | \forall T_k \in C_k), 1 \leq k \leq n$. Data discretization processing and feature selection are completed through training, that is, data preprocessing is realized. In the preprocessing, the effective data is filtered out, the prior probability $P(T_k|C_k), k = 1, 2, \cdots, n$ is obtained according to the statistical results, and the centralized data set is determined through the mapping relationship, so

that the internal safety behavior of the entire car driving identification system can be analyzed. In the second stage, the data in the whole frame is extracted, and the extracted data of the car driving identification system is visualized by the idea of discretization and feature selection, and the internal redundant data and unimportant feature data are simplified. By reducing the time complexity and space complexity of the safety of the car driving identification system, the accuracy of the safety of the car driving identification system can be improved [7].

3 Car Driving Identification System Communication Abnormality Safety Data Strength Identification

In order to better deal with heterogeneous data, the data strength of abnormal communication safety of the automatic identification system for navigation is identified. Security data strength identification is divided into three parts: data collection, security analysis and response processing. The data strength identification structure of system communication anomaly security is shown in Fig. 2.

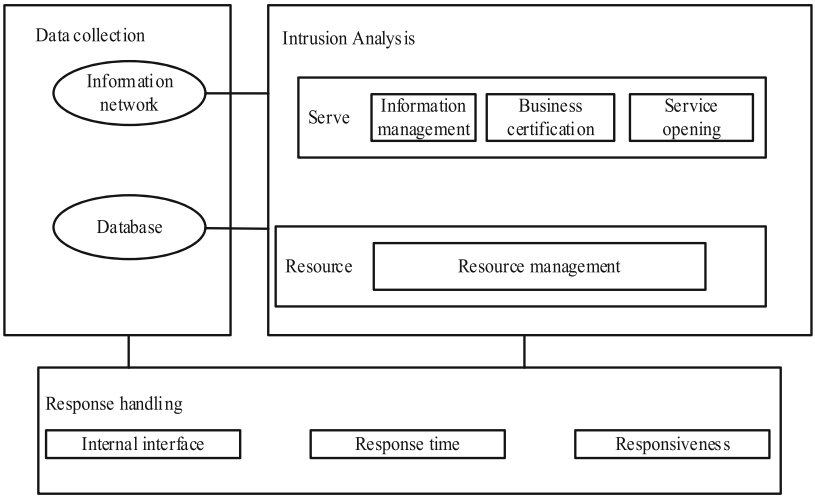


Fig. 2. System communication abnormal security data strength identification structure

According to Fig. 2, data collection is the collection of heterogeneous data, which is the basis of safety analysis. Security analysis is a core step in deep learning analysis methods. It processes the collected data and compares it with the original data to determine whether the data is normal and safe and whether it affects the overall operating state. If the data is abnormally safe, an alarm will be issued through response processing, and the on-duty personnel will extract the data through the original data stream and compare it with the stored data for correction. The deep learning analysis is carried out by integrating the information of the main car driving identification system and the information of several diversity engine car driving identification systems. According to

the trajectory of heterogeneous data, its safety behavior is found, and the normal sample of the host is compared with the analyzed data sample, and the heterogeneous data is corrected to ensure the accuracy of system resources [8].

Therefore, in the identification of data intensity, it can be classified according to the analysis object and security method, and can be divided into two categories according to the difference of the analysis object. The main engine data and the car driving identification system data are divided into two types of security methods: abnormal data and input errors according to different security methods. The classification of safety data is shown in Table 1.

Table 1. Classification of safety data

Classification basis	Classification result
Analysis object	Host data
	Car driving identification system data
Security way	Data exception
	Input error

In order to minimize data security, try to avoid errors when inputting computer programs, reduce system errors, and improve system accuracy. Classify the security methods of data anomalies, discover data anomalies and input errors in time, and avoid the impact on later data.

According to the log and display data, the known abnormal data is turned into an attack code pattern and stored in the security simulation database. Then match the real-time correct data with the abnormal data in the security schema to identify the security data. The data encoding method is shown in Fig. 3.

4 Build a Heterogeneous Data Processing Model

Because in the Cartesian coordinate system, the abnormal data samples and the normal data samples are inconsistent, so this paper completes the data processing work by establishing the Cartesian coordinate system and constructing the heterogeneous data processing model. Randomly select n data as the basic sample, draw the ROC curve through Matlab software, determine the exact value of the data, and repeat this operation. Sampling other samples to calculate the offset between the standard data and the measured data, storing the coincident data, and rechecking and integrating the different data until the ROC curve is a coincident line [9]. The established Cartesian coordinate system is shown in Fig. 4.

The vertical axis of the ROC curve represents the analysis probability, and the horizontal axis represents the false alarm rate. According to the change of the curve, the false alarm rate is analyzed. The higher the threshold, the higher the accuracy of the system and the stronger the self-identification ability. If the ROC is not a smooth curve, the ROC curve needs to be divided into several segments to form several small trapezoids,

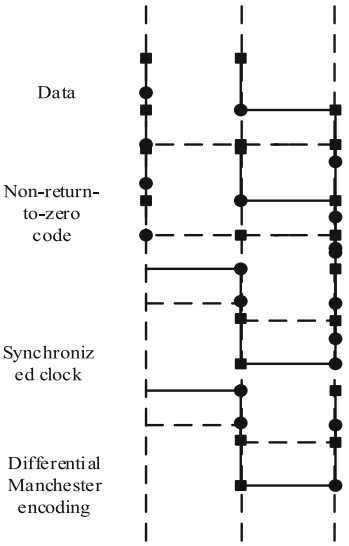


Fig. 3. Data encoding method

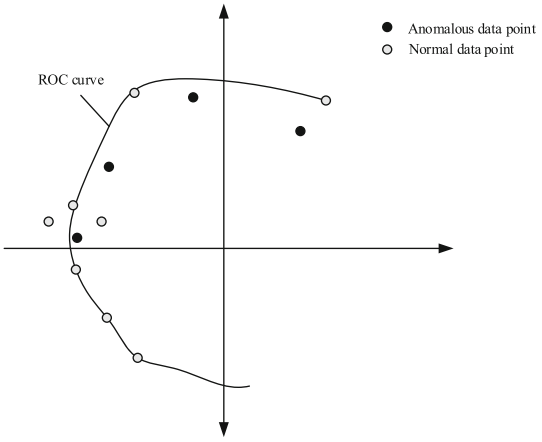


Fig. 4. Data processing cartesian coordinate system

and the area of each trapezoid is calculated as the exact value of the data. By adding several trapezoidal areas, the number of data is subtracted from the number of normal data, and the false alarm rate of abnormal data is obtained. The optimal working point of the analysis was found in the ROC curve, and the positive likelihood ratio and Youden index were used to discriminate the error detection rate and the false alarm rate.

Looking at Fig. 4, it can be seen that some abnormal sample points may be generated due to operational errors in system communication. In general, the isolated points that do not coincide with the ROC curve made are obtained due to operational errors. Therefore,

in order to ensure the accuracy of the data, we must first ensure the accuracy of the data in the host system, correct the irregular data, and mark the heterogeneous data [10].

The networking of the car driving system is periodic, and each program is arranged in the order of abnormal data attack. According to different programs and different environments, call the program. In the car driving identification system, each node corresponds to a different program, and each path inside the program represents the process of each data transmission. Establish different data transmission channels to form a data network, implant deep learning analysis systems and alarm systems, and conduct security deep learning analysis under certain security strategies. Since each path in the car driving identification system has a starting point and an ending point, and has the function of storing data on the node, abnormal data often attacks each node through the loopholes in the program. By changing the data transmission path of the source program, the overall sequence is different from the normal execution sequence. Therefore, in the process of data processing, this paper builds a heterogeneous data processing model:

$$E(n) = \frac{1}{2}\sum_{j=1}^{J} e_j^2(n) \tag{5}$$

Among them, e is a constant value, and n is the number of abnormal data detected.

5 Security Data Deep Learning Analysis

Deep learning analysis methods are mainly divided into five stages: database cleaning and integration, database storage, selection and transformation of specific data sets, data mining to form patterns, and evaluation and representation. The security data deep learning analysis process is shown in Fig. 5.

Observing Fig. 5, it can be seen that the role of database cleaning and integration is to find abnormal data and integrate and clean the abnormal data. The role of database storage is to store the cleaned data and combine the data in the data source. The function of selecting and converting a specific data set is to filter and integrate the integrated data into a data package for specific storage. The data mining formation mode is to decompose the specific stored data, and the data is decomposed regularly. The function of evaluating and representing knowledge is to filter out meaningful pattern knowledge based on the decomposed data, and display it to the user by using the visualization of the data.

The data is transmitted through the transmission network, and the small central processing unit at the end of the node reads, audits and records the data, analyzes it with the exevce/inetd system, generates new data, and the host system identifies the data itself. If the data is abnormal, return to the beginning, picket and retransmit the data. If the data and the original data continue to be transmitted downward, the data value of the path is obtained, and it is judged whether it is a correct program. If it is not reprogramming, if the data is weighted, the corresponding service privilege vector is obtained, and it is judged whether the PID exists in the vector. If it is not present in the vector, the system needs to be reprogrammed. If it exists in the vector and continues to transmit downwards, it is judged whether it is fork. If it continues to transmit to the

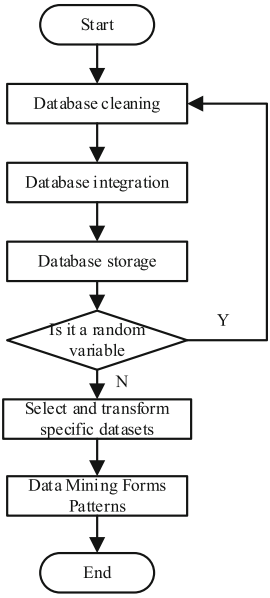


Fig. 5. Security data deep learning analysis process

background, the output data will be stored in the corresponding data repository. If not, the data needs to be checked and corrected for retransmission.

In this paper, the original data is mapped into the three-dimensional space by constructing a linear function, and the space is divided. The optimal solution is obtained by using the matrix to find heterogeneous data, and the minimum error average criterion E = 1 is adopted. Divide the overall data set into non-overlapping data blocks, so that the overall data forms a compact independent body. The segmentation process is shown in Fig. 6.

The data independent body is obtained according to the data segmentation principle in FIG. 6. After obtaining the discrete attribute data, the original data is mapped into the three-dimensional space by constructing a new linear function. Divide the space and use the matrix to find the process of heterogeneous data to obtain the optimal solution. The deep learning analysis method mainly relies on the simulated database. If there is no normal data in the simulated database, the attack data cannot be analyzed. If the real-time encoding of the abnormal data and the normal data exceed a certain threshold, the normal data will also be attacked. The overall data is analyzed and processed to show the nonlinear relationship between normal data and abnormal data. The data is compared by random sampling, the HMM model is established, and the analysis function of the HMM model is used to identify abnormal data through the deep learning test, realize the distributed processing of information, and increase the adaptability of the processing process. The HMM model construction is shown in Fig. 7.

Observing Fig. 7, it can be seen that the data transmitted on each channel can be referred to as a data stream, which has the characteristics of continuity, large capacity, and fast response. When heterogeneous data security, deep learning analysis is performed in

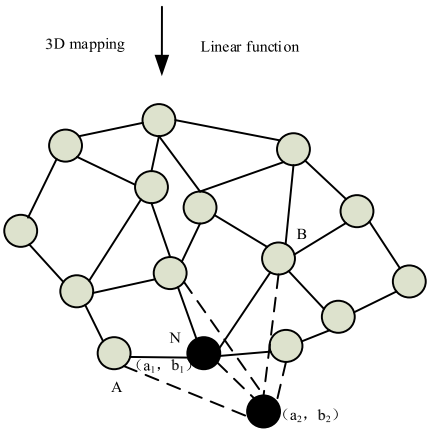


Fig. 6. Principle of data segmentation

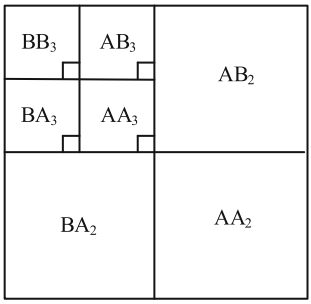


Fig. 7. HMM model construction

the data stream, if the data is part of the event data, it is security data. There are three main types of data: point anomalies, sample anomalies, and sequence anomalies. The transmission data of the sensing data stream enhances the stability of the data stream algorithm, improves the analysis performance, and increases the stability of the analysis process.

6 Car Driving Identification System Security Data Defense Control

The core concept of deep learning is to combine a variety of big data technologies to realize the functions of collecting, processing, analyzing, storing and retrieving massive data. In order to realize the precise defense control of the safety data of the car driving identification system. Based on deep learning, this paper performs stream processing and data mining on safety data by accessing system operation data to achieve high-efficiency, low-latency, and high-accuracy car driving identification system safety data defense control.

The workflow of the safety data defense control of the car driving identification system based on deep learning is shown in Fig. 8.

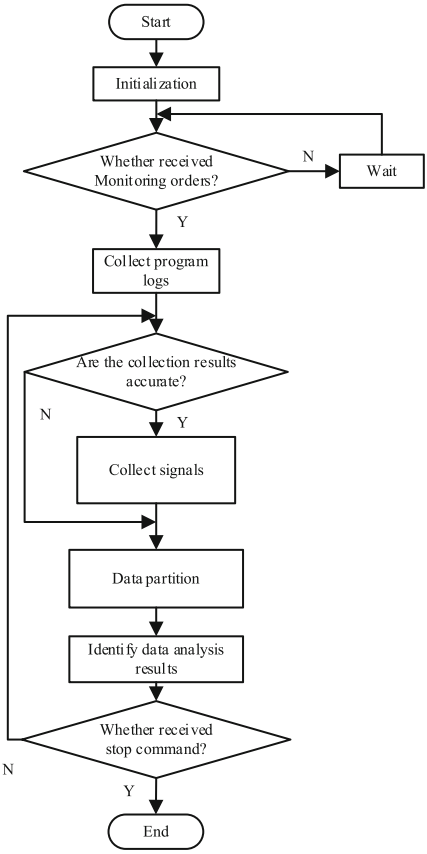


Fig. 8. Security data defense control process of car driving identification system

(1) The host detector collects the operating data of the host operating system and the log of the application program. The data packets of the car driving identification system are obtained by the network detector. Identify the security data according to the corresponding security rules, and perform simple data processing on the data. When the safety data is analyzed, the alarm mechanism is activated to send the safety information to the central processing unit.

(2) After the central processor receives the alarm signals and safety data from different detectors, it divides the safety data into R data sets X based on the principle of deep learning, and performs classification data training on the generated data sets.

Using meta-classifiers to mark security data, assuming that a certain representation data is a, the labeling result of the r meta-classifier for data a can be expressed as:

$$G(a) = b \sum_{r=1}^{R} sign\left(g_{r(a)} = b\right) \tag{6}$$

where, $G(a)$ is the labeling result, *sign* is the indicator function, $g_{r(a)}$ is the unlabeled data, and b is the labeling coefficient. When $g_{r(a)} = b$, *sign* value is 1, otherwise it is zero.

Calculate the confidence of the marked security data a as follows:

$$con(a) = \frac{1}{R}\sum_{r=1}^{R} sign\left(g_{r(a)} = b\right) \tag{7}$$

Considering the noise pollution carried by the security data, a generalization error algorithm is introduced to estimate the generalization error of the confidence error. The calculation method is as follows:

$$u = \frac{1}{n}\sum_{(a,b)} nsign(con(a)) \tag{8}$$

Among them, n represents the number of data contained in the dataset X, and u represents the generalization error. According to the above error estimation, if the error value is greater than 1, the confidence calculation needs to be recalculated. If it is smaller, it means that the error is not enough to affect the final calculation result, which can be ignored and the next step is calculated.

(1) Select the confidence threshold. According to the above confidence calculation results, the optimal threshold for high confidence and the optimal threshold for low confidence are selected to be represented by ε_1^r and ε_2^r, respectively. The selection of the confidence threshold affects the efficiency of data analysis. The optimal threshold for high confidence and the optimal threshold for low confidence should satisfy the following relationship:

$$\varepsilon_1^r = \frac{1}{\varepsilon_2^r} \tag{9}$$

(2) Divide the data according to the confidence threshold of the data, and divide the security data whose confidence is higher than the optimal threshold of high confidence into the training sample set, and perform data training on them. Analyze the correlation between data and extract security rules from the rule base, so as to clarify the types of security data. For the safety data whose confidence is lower than the optimal threshold of low confidence or between the thresholds, it is put back into the data set X, and the next data calculation is performed.

(3) Match the appropriate defense mechanism from the database according to the identification result of the security data. The control unit of the central processing unit issues control instructions to control the operation of the corresponding defense mechanism. The data results and information of this time are stored in the memory to realize data analysis, which is convenient for the next safety signal analysis.

The confidence degree of safety data is calculated by marking the safety data, and the generalization error is calculated by using the generalization error algorithm to calculate the optimal threshold, match the appropriate defense mechanism, and complete the defense control of the safety data of the vehicle driving recognition system.

7 Experimental Studies

In order to verify the effectiveness of the safety behavior analysis method of the car driving identification system based on deep learning proposed in this paper, a comparative experiment was set up to compare with the method of reference [2] and the method of reference [3] respectively.

The experimental data selected in this paper comes from the KDDCUP security analysis data set. The internal data sources of the KDD security analysis data set mainly include two parts:

(1) Seven weeks of training data, about 5,000,000 connection records of the automatic identification system for car driving.
(2) Abnormal attack type. There are 22 types of attacks, which can be specifically divided into four main types of attacks. The description of exception types is shown in Table 2.

Table. 2 Description of abnormal types

Type of attack	Description of attack
Probe	By monitoring or scanning the port, the attack type of the attack is realized
R2U	Attack the process host and count all unauthorized access
U2R	Analyze unauthorized local user access methods
DOS	All denial of service attacks

The experimental process is shown in Fig. 9.

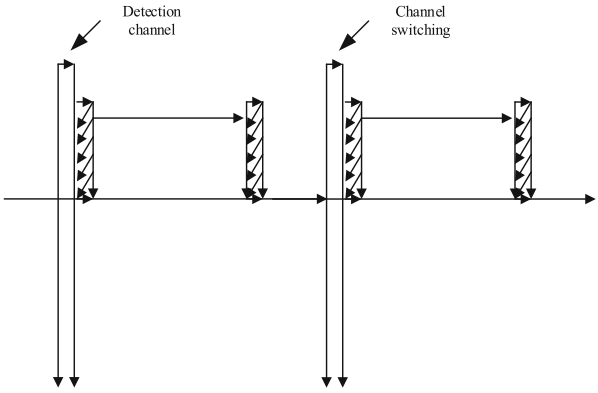


Fig. 9. Analysis of the experimental process

The set experimental parameters are shown in Table 3.

Table 3. Experimental parameters

Parameter	Project
Operating system	Windows10
CPU frequency	5.2GHz
Memory	5GB
Hard disk storage space	200G
Programming tools	MATLAB8.0
Test analysis method	Trs/Tes

Fig. 10. Build experimental environment

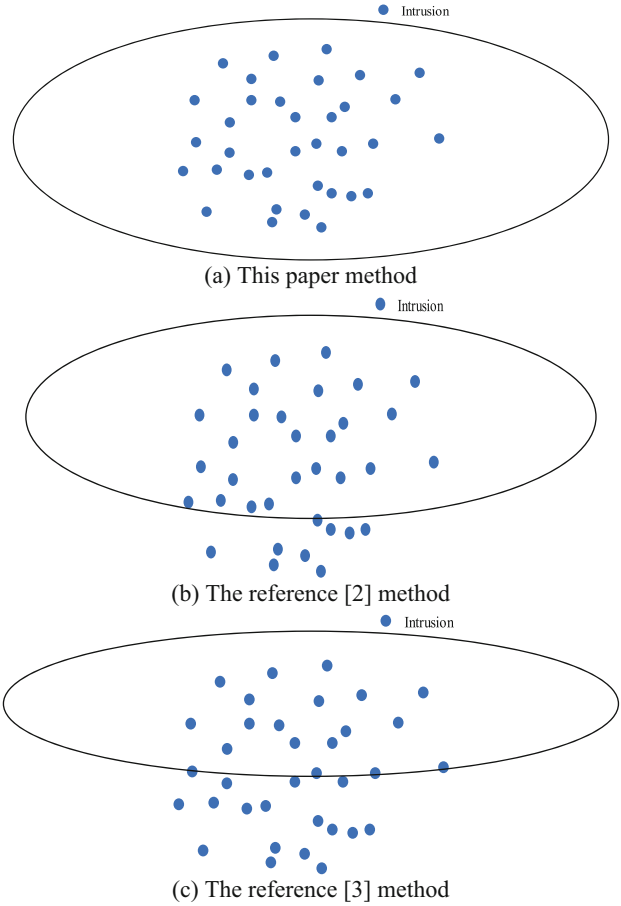
Build experimental environment is set as shown in Fig. 10.

Experiments were carried out according to the above experimental parameters and experimental environment, and the safety analysis capabilities of different methods were compared. The analysis results obtained are shown in Fig. 11.

According to Fig. 11, compared with the method of reference [2] and the method of reference [3], the method in this paper has strong information matching ability. It can match all safety behaviors and accurately analyze all safety types, so as to realize behavior analysis. Because the training sample value inside the method in this paper is continuously expanded, the error of the conditional probability is gradually reduced, the continuous learning ability and expansion ability of the method itself are improved, and the security analysis ability is enhanced.

After determining the safety analysis capability, the safety analysis matching range of different methods is shown in Table 4.

It can be seen from Table 4 that the security analysis range of the method in this paper is much larger than the security analysis range of the method of reference [2] and the method of reference [3], which can realize the analysis and matching of data. Its



(a) This paper method

(b) The reference [2] method

(c) The reference [3] method

Fig. 11. Security analysis capabilities of different methods

matching range is large and can match all security behaviors. Because this method uses the generalization error algorithm to calculate the generalization error, thus obtaining the optimal threshold, which can match the appropriate defense mechanism and improve the range of security analysis.

The safety analysis error rate results of different methods are shown in Table 5.

It can be seen from Table 5 that the security analysis error rate of the method in this paper is significantly lower than that of the method of reference [2] and the method of reference [3]. Therefore, the method in this paper adopts deep learning analysis to better analyze the data and explore the internal strength of the data, thereby reducing the error rate of security analysis.

Table 4. Safety analysis matching range of different methods

Scope	The reference [2] method	The reference [3] method	This paper method
Decision tree	Cannot match	Can match	Can match
Support vector machines	Cannot match	Cannot match	Can match
Manual car driving identification system	Cannot match	Can match	Can match
Neural car driving automatic recognition system	Can match	Cannot match	Can match
Genetic algorithm	Cannot match	Can match	Can match
Data information	Can match	Cannot match	Can match
Car driving identification system information	Cannot match	Can match	Can match
Car driving identification system attack	Can match	Can match	Can match
Safe sex	Can match	Cannot match	Can match

Table 5. Safety analysis error rate results of different methods

Different methods	Security analysis error rate
The reference [2] method	3.6%
The reference [3] method	2.5%
This paper method	0.8%

8 Conclusion

In this paper, a deep learning-based safety analysis method for automatic identification of car driving is proposed, and a safety analysis model of automatic identification of car driving is established based on deep learning, and a heterogeneous data processing model is constructed through the identification of abnormal safety data intensity of communication. Based on the deep learning analysis process of security data, access system operation data, stream processing and data mining of security data, complete system security data defense control, and realize system security analysis. The experimental results show that the method has strong security analysis ability, large matching range and low security analysis error rate. However, in this study, only a relatively rough analysis of the automatic identification system for automobile driving has been made, and the processing of automatic identification has not been realized by programming. In the

future research, the research results of this time need to be applied to practice and constantly improved, so as to improve the safety performance of the automatic identification system for automobile driving.

Acknowledgement. 1. Science and Technology Youth Program of Chongqing Education Commission in 2020:Design of A pillar blind zone vision system for passenger cars (Project No.: KJQN202004602).

2021 Chongqing Vocational Institute of Tourism Mass Innovation Space Project:Universal Vision Given by Science and Technology -- Development of Visual System for Blind Zone of Passenger Car A Pillar (Project No.: 2021DC01).

References

1. Sun, X., Shi, W., Cheng, Q., et al.: An LED detection and recognition method based on deep learning in vehicle optical camera communication. IEEE Access **9**, 80897–80905 (2021)
2. Chu, N., Zhang, S., Gao, Y., et al.: Safety analysis method of aero-engine systems based on Simscape model. J. Aeros. Power **36**(04), 885–896 (2021)
3. Yang, H., Sun, Y., Ruan, H.: Research on safety assessment method for IMA system based on AADL and HiP-HOPS. Aeron. Comput. Techn. **49**(06), 85–88 (2019)
4. Alzubi, O.A.: A deep learning-based frechet and dirichlet model for intrusion detection in IWSN. J. Intell. Fuzzy Syst. **42**(2), 873–883 (2022)
5. Wang, Z., Liu, Y., He, D., et al.: Intrusion detection methods based on integrated deep learning model. Comput. Secur. **103**, 102177 (2021)
6. Lu, J., Liu, X., Zhang, S., et al.: Research and analysis of electromagnetic trojan detection based on deep learning. Secur. Commun. Netw. **2020**(4), 1–13 (2020)
7. Riyaz, B., Ganapathy, S.: A deep learning approach for effective intrusion detection in wireless networks using CNN. Soft. Comput. **24**(22), 17265–17278 (2020)
8. Mallick, M., Chang, K.C., Arulampalam, S., et al.: Heterogeneous track-to-track fusion in 2D using sonar and radar sensors. In: 2019 22th International Conference on Information Fusion (FUSION), pp. 1–8. IEEE (2019)
9. Singla, J.: Comparing ROC curve based thresholding methods in online transactions fraud detection system using deep learning. In: 2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), pp. 9–12. IEEE (2021)
10. Sufen, L., Xueli, Y.: Mathematical modeling and simulation of data buffer replacement algorithm in heterogeneous network. Comput. Simul. **38**(12), 286–290 (2021)