Design and Implementation of Intrusion Detection System Based on Data Mining

Xin Li

Beijing Communication University of China, Beijing, China

Keywords: Data mining technology, Intrusion detection system, Database design, System module design

Abstract: The problem of network security is related to the intrusion of the hacker and the virus to some extent, which is not conducive to the healthy operation of the computer network system. This paper expounds the construction of the intrusion detection system model based on the data mining technology, and the design and implementation of the detailed analysis system, which is to lay the foundation for the smooth progress of the research work in the future.

1. Introduction

The continuous updating of Internet information technology promotes the development of data mining technology, pays attention to strengthening the construction of intrusion detection system model, and fully combines theoretical knowledge with practical experience in the specific operation link, improves the development quality and level of information technology products, and takes improving the accuracy of intrusion detection technology as the research focus to meet the needs of the development of current data mining technology.

2. Intrusion Detection System Model Based on Data Mining Technology

The intrusion detection system model based on data mining technology mainly includes system model design, intrusion detection method model design, database mining algorithm model design and so on. Data mining and intrusion detection should be fully considered in the design process of system model. Among them, the data acquisition is mainly to integrate the daily data information, responsible for the collection of receipts, real-time monitoring of the current operation of users. Data preprocessing is mainly to unify the data processing in the process of data acquisition. Data mining is mainly to give full play to the advantages of the algorithm, scientific analysis of relevant data information, and in the process of building a rule base, to extract data The characteristics of behavior are the starting point. The establishment of rule base mainly saves the behavior of users and divides it into normal and abnormal. Intrusion detection is mainly to detect the behavior of users, and the behavior of intrusion is detected by means of anomaly and misuse. Response refers to the timely alarm for abnormal behavior, which lays the foundation for the smooth progress of the follow-up operation. The detection efficiency of the system is high, and its adaptive ability is strong based on its intelligent advantages.

The model design of intrusion detection method needs to define the intrusion mode, detect it with the help of misuse and anomaly detection method, and monitor the intrusion behavior in real time. The accuracy of the detection method is high, and the feature database is compared, but there is still a phenomenon of missed detection in the actual detection link. In the link of distinguishing normal data from abnormal data, it is necessary to combine misuse detection and data mining algorithm organically to detect whether there is intrusion phenomenon in user behavior, which is helpful to improve the efficiency of intrusion detection.

The model design of data mining algorithm mainly gives full play to the advantages of clustering technology to analyze and judge the audit data and screen out the abnormal data. The intrusion standards are compared with the pattern rule base, for example, when some users access a fixed database for a long time, the behavior rules of the user will be formed, and the legitimate behavior

  DOI: 10.25236/iiicec.2019.026

will be judged by the model rule base. Among them, the advantages of association analysis algorithm are obvious, and the classification and integration of data information is carried out to find out the law, which provides support for the establishment of rule base. For example, K-Means algorithm is a kind of clustering algorithm, which processes information quickly and will normal data. It is easy to understand and reduce the difficulty of work by filtering the associated shared items in abnormal data search.

3. Design and Implementation of Intrusion Detection System Based on Data Mining Technology

3.1 Overall Design of Intrusion Detection System

The overall design of the intrusion detection system mainly includes the overall system design goal, the system function module design, the system flow design and so on. The overall design goal of the system is integrated with the data information acquired by the advantages of the data mining technology, the behaviour characteristics of the users are acquired, the detection and the abnormal detection are detected by means of misuse detection, and the flexibility of the rule base of the intrusion detection system is emphasized, Establish and perfect the perfect intrusion detection system. The system function module is designed to ensure the reliability of the data in the process of data pre-processing, obtain the data source in the audit log and sort it so that it can be standardized. The data mining module mainly relates to the clustering algorithm and the correlation algorithm. The data volume in the database is detected, the similarity of the clusters is distinguished by the clustering algorithm, and the normal data is screened out, and the detection is carried out by using the Apriori algorithm. The rule base is divided into a normal library and an exception library, and the rule base is uniformly managed. In the process of intrusion detection, the alarm notification shall be collected in real time to prevent the problem of leakage detection. The system flow design is to pre-process the collected audit log and perform cluster analysis in the data mining module. Compare with the behavior rules in the abnormal database in the detection link. In case of abnormal behavior, a warning will be issued, the data without alarm will be associated and analyzed. The behavior is mined by means of data mining technology, and compared with the normal database. If the alarm is not issued, it is normal behavior, and the abnormal data found in this section shall be handed over to the professional personnel.

3.2 Database Intrusion Detection System Database Design.

The design of intrusion detection system database mainly includes conceptual design and logical design. Conceptual design needs to master the relationship between entity and attribute, optimize the structure model of concept, draw the entity relation diagram according to the actual situation of database intrusion monitoring system, and lay the foundation for the follow-up research work. In the process of intrusion monitoring, the intrusion time, user, operation and geological information of intrusion alarm are worked out and submitted to technical personnel for processing. Logical design needs to clarify the user information table, where the table mainly includes fields, data types, instructions, and whether or not the primary key several The two data types of USERNAME,PASSWARD, are VACHAR (20). The user name and password are mainly included in the description, and whether the primary key is yes or not. The fields in the audit data initialization table mainly include eight fields, in which ID indicates that the session ID,USERNAME represents the user name, TIMESTAMP is the timestamp, OPTION represents the operation name, OBJECT-NAME represents the operation object name, RESCODE is the operation return code, and HOST is the client terminal ID,FLAG. Abnormal data identification, remarks information mainly includes primary keys and non-empty. The field RULEID in the user behavior rule table represents the support of the rule ID,SUPPORT, and the CONFINDENCE,RULR represents the confidence and the rule respectively, in which the first field is the primary key and the other three are non-empty. The exception behavior rule table mainly includes seven fields, in which RULEID,RULE-NAME represents the rule ID, rule name, USERNAME,OBHECT-NAME

represents the user name and action object name, and HOST represents the rule name. Is the client terminal name, and TIME-CYCLE,THRESHOLD represents the time interval and threshold, the first rule ID as the primary key, the other six are non-empty [1].

3.3 Design and Implementation of Function Module of Intrusion Detection System.

The design and implementation of the function module of the intrusion detection system mainly includes the data pre-processing module, the data mining module, the rule base generation module, the intrusion detection module and the response module. The data pre-processing module mainly includes two parts of data acquisition and processing. In the process of data processing, the integrity of data information is to be ensured, and the deficiency of the data is supplemented to help improve the efficiency of the algorithm. The validity of mining information is guaranteed, and the data is converted into Boolean data, which mainly includes static association rules, Boolean association rules and distance association rules. In the data mining module, there are two kinds of clustering analysis and association analysis, in which the clustering analysis is mainly analyzed with the help of K-means clustering algorithm, and its criterion function formula is as follows: In the rule base generation module, $J = \sum_{i=1}^{k} \sum_{p \subset Ci} \left| P - m_i \right|^2$ it is necessary to establish and manage the normal behavior rules and abnormal behavior rules, in which the support degree of the normal behavior rules is 60%, 40%, 30%, the confidence level is 60%, 80%, 80%, the adaptability of the abnormal behavior rule base is poor. It is necessary to pay attention to the updating and optimization of the rule base in the actual operation link, which is helpful to ensure the system adaptability of the rule base. Intrusion detection module mainly includes Misuse detection and anomaly detection can monitor the user's operation behavior in real time in the link of misuse detection, set the threshold for the number of operation failures, and alarm the intrusion behavior. Anomaly detection integrates the collected exception data, classifies the associated information with the help of data mining technology, compares the user's operation behavior with the normal behavior rules, sends an alarm when the intrusion occurs, records the alarm information, and processes it by the professional technical personnel. The function of response module can effectively reduce the loss of database, prevent intrusion behavior in time, and generate form of the report hand over to the database manager [2].

4. Conclusion

The design and implementation of intrusion detection system based on data mining technology includes many aspects, including the overall design of intrusion system, the design of system database and the design and implementation of system function modules. Based on the requirements of intrusion detection system, attention is paid to the optimization and improvement of intrusion detection module, which is helpful to ensure the safe operation of database.

References

[1] Wang, Li. (2018). Network database intrusion detection system based on data mining. Computer knowledge and Technology, vol. 14, no. 36, pp. 7-8.
[2] Su, Xin. (2018). Design and simulation of adaptive intrusion detection system based on data mining. Yangzhou University.