

# *Campus Security Access Control System Relying on Association Rules*

Qingwei Wang\*

*School of Physical Education, Harbin Huade University, Harbin 150025, China*

*wangqingwei1217@163.com*

*\*corresponding author*

**Keywords:** Association Rules, Campus Security, Access Control System, Alarm Model

**Abstract:** There are many students in colleges and universities, and most of them are in the open state. The social people can enter and exit in colleges and universities, and the financial and personal safety of students and teachers can not be well guaranteed. The purpose of this paper is to study the campus security access control system based on dependency association rules. This paper introduces the background and research significance of the campus security management system, describes the status quo of the combination of access control data and campus security, and designs the system functions according to the characteristics of access control data, including personnel data management, access data management. Base station alarm association rule mining model is put forward, and then extracted from the base station alarm database part of data mining, data preprocessing been done according to the characteristics of the alarm data mining transaction database, the experimental results show that with this article campus entrance guard alarm correlation mining model alarm transaction database mining which can obtain meaningful alarm rules.

## 1. Introduction

The access control system has been widely applied in many scenarios, such as security, transportation, education, medical treatment, police, e-commerce, and so on, showing significant application value [1-2]. As the core application of campus digital security, the access control system is gradually being applied in many campuses, which greatly reduces the threat from criminals outside the campus, thus ensuring the safety of campus people, money and property [3]. However, the existing access control system is missing in security prevention for the abnormal or security threats of campus personnel themselves, such as students' abnormal behavior, staying out at night, skipping class or missing, etc. In addition, with the gradual increase of access control system, there

is a lack of effective means to deal with the incoming and outgoing data generated by massive personnel in the system and the constantly updated data form, and there is a lack of intelligent security application in the use of data, which cannot meet the security needs under the new situation [4-5].

Access control system is the management of the door control, is a management personnel in and out of the security application equipment system, the access control system designed by Sujit Biswas is to identify the Mifare S50 IC card number as close to the RFID high-frequency reader sensor area, and then compare the data with the database. Finally, the opening and closing of the electronic lock is controlled by AT89C52 microcontroller through the control relay. The design steps include requirement analysis and determination of the necessary system functions, the selection of high-frequency radio frequency card, reader and MCU hardware models, and then software design; Finally, the normal communication between each module is debugged to realize the scheduled function [6]. Amit Kumar Sikder designed a library access control and reader analysis system based on fingerprint recognition technology, WIFI wireless transmission technology and Internet of Things (iot) technology in Yangon University Library. The system can collect and compare fingerprints in the lower computer system, and transmit relevant access information to the upper computer system through WIFI. The system manages the basic data and provides multi-angle query statistics for access information [7]. Padmavathi Iyer proposed a method for extracting regional evolution interpretation/prediction models based on association rule mining. In order to deal with the asymmetry of the learning data used, they suggested to adjust the support allocation process of MSApriori and proposed a new algorithm, called BERA[8]. Therefore, the development of access control system is of great practical significance for ensuring campus security and improving the information management level of schools [9].

This paper discusses the source of the subject, the current situation of the school's information construction, the current situation of the research field of access control system and the problems existing in the process of access control system construction. The introduction of the relevant theory and development technology used in the development, determine the actual needs of the school so as to determine the system in the development of the function to be completed. This paper summarizes the work of this system and the characteristics and function of the significance of the system, but also pointed out the development direction of access control technology.

## **2. Research on Application of Campus Security Access Control System Relying on Association Rules**

### **2.1. System Configuration Module**

The purpose of system configuration is to set some necessary parameters, such as initialization parameters, anomaly detection parameters, etc. In the design of this system, the initial configuration is divided into four parts, namely, initialization configuration, dormitory security configuration, message center configuration and behavior anomaly configuration, as shown in Figure 1. The initial configuration is mainly to configure the database address, user name and password. Dormitory security configuration is mainly to configure the abnormal time in the dormitory; The message center configuration configures whether to display abnormal messages. Abnormal behavior configuration is to configure the abnormal threshold parameters in the abnormal behavior detection module [10-11].

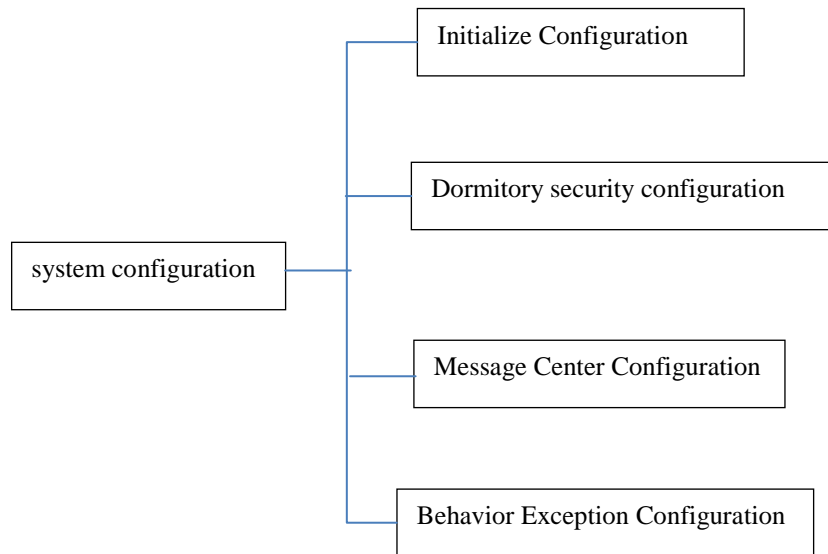


Figure 1. Schematic diagram of system configuration functions

## 2.2. Design of Data Management

### (1) Personnel data management

In this system, the personnel data management module is functionally divided into displaying personnel data, downloading personnel information template, uploading personnel data, editing and deleting personnel data [12]. Display personnel data refers to the persons on uploading data visualization display, such as personal name, student number, id number, phone number, email, download template refers to upload information personnel information when required by the template, because this system on the personnel information data recorded by excel format input, so you need to follow a certain format and specification, Therefore, this template is designed; Uploading personnel data is to upload personnel information in batches through excel sheets. Edit and delete the uploaded personnel information, and if there is any error, it can be modified [13-14].

### (2) Incoming and outgoing data management

In the design of data in and out of a total of two functions are data interface and data display. Data interface refers to the acquisition of incoming and outgoing data through the form of interface. There are two ways to design the interface: one is to upload incoming and outgoing data through visual buttons in the form of txt files; the other is to upload data through API in the form of programming; Data display is a visual display of uploaded data [15-16].

The data management page is divided into two parts. The upper part is the function button to download the entry and exit data template and upload the entry and exit data respectively, while the lower part is the display of the entry and exit data, including serial number, name, certificate number, entry and exit time, entry and exit status, entry and exit device, device type, entry and exit area, and body temperature [17].

## 2.3. Association Rules

The basic concepts of association rules include transaction, item set, support degree, confidence degree, frequent item set and infrequent item set, association rule, strong association rule, etc. [18].

Support(s): The ratio of the number of occurrences of transactions containing certain itemsets to

the total number of data sets. If the support degree of X and Y is analyzed, it is defined as:

$$\text{support}(X, Y) = P(XY) \frac{\text{number}(XY)}{\text{number}(ALLSamples)} \quad (1)$$

Confidence(c): The ratio of Support(X, Y) and Support(X), defined as:

$$\text{Confidence}(X \leq Y) = P(X|Y) \frac{P(XY)}{P(X)} \quad (2)$$

The method to discover the original association rules is to use enumeration method, that is, by finding out all possible candidate itemsets, including many infrequent itemsets, and then comparing the support degree of candidate itemsets with minsup, the frequent itemsets are retained. This method is time-consuming and inefficient.

Using the principle of Apriori algorithm, deleting part of the candidate item sets is equivalent to pruning the data set. After pruning, the candidate item sets become less, and the operation efficiency is greatly improved compared with enumeration method. The Apriori algorithm process is as follows:

In the first step, data sets were scanned. Firstly, the support degree of each item was calculated according to the number of data sets, and then item sets greater than or equal to minsup were retained to obtain frequent 1- item set L1.

In the second step, the set generated by L1 is pruned to generate the set C2 of candidate 2- itemsets, and each item in C2 is counted. Retaining items greater than or equal to minsup, obtaining frequent 2- itemset L2;

In the third step, by analogy, the set generated by Lk-1 is pruned to generate the set Ck of candidate K- itemsets, and then the items greater than or equal to minsup are retained to obtain frequent K- itemsets. Until finally no new frequent itemsets are generated, the rules with greater than or equal to the minimum confidence are retained.

### 3. Investigation and Research on the Application of Campus Security Access Control System Relying on Association Rules

#### 3.1. Campus Access Alarm Association Mining Model

According to the process of data mining according to the characteristics of the campus entrance guard the alarm data, set up warning model for mining association rules mining, a complete mining association rules including the base station of alarm data acquisition, the campus entrance guard alarm data pretreatment, the campus entrance guard alarm association rule mining, association rules analysis and post-processing, rules of application of these processes.

There are a large number of redundant, incomplete and repeated alarm data collected from the original campus access control alarm database. If it is directly used to mine association rules, not only the mining efficiency is low, but also the obtained rules can not reflect the real situation. Therefore, the collected alarm data must be preprocessed, including redundancy processing, field information processing, data normalization processing, and time segmentation processing. The preprocessed alarm data is used to form the alarm mining transaction database. The Apriori algorithm is used to mine the alarm transaction data. The rules obtained by mining are analyzed and post-processed to get meaningful rules. These meaningful rules can be applied to the management of campus access alarm.

### 3.2. Alarm Data Extraction

The alarm data used in this article is from the database station of Campus Security Access Control System, which stores historical alarm information. The name of the table for storing historical alarms in the system database is alarmTmp. For research purposes, 618429 historical alarm data of the whole two months from 2021-09-01 00:00:00 to 2021-10-31 23:59:59 are extracted from this table.

## 4. Analysis and Research on the Application of Campus Security Access Control System Relying on Association Rules

### 4.1. Deleting Duplicate Alarm Data

Duplicate alarms occur because an exception is detected by related nes and each NE sends the exception alarm. In the alarm\_datasource table, if all fields are the same except the ID, the alarm data is a duplicate alarm. You only need to save one duplicate alarm. To delete a duplicate alarm, perform the following steps:

```
for(i=0;i<count(alarm_datasource)-10;i++)
    {
        for(j=i+1;j<i+10;j++)
            {
                If(The fields are identical except for ID)
                    Delete the record
            }
    }
```

Based on the observation of alarm data, most duplicate alarm data are stored side by side because the alarm time is the same. Therefore, check the last 10 alarms of one alarm data and delete the 10 duplicate alarms.

### 4.2. Normalization of Data

For data normalization purposes, we use numbers to represent levels uniformly here, with the number 1 replacing urgent or critical, 2 replacing important or major, 3 replacing general or minor, 4 replacing warning or waring, and 5 replacing uncertainty or uncertain. We also need to normalize the data in the alarmncatalog field. Run the distinct operation on the data in the alarmncatalog column to query all types of the alarmncatalog field. All types of alarms are coded as shown in Table 1. The segment codes of alarm time are shown in Table 2.

*Table 1. Alarm type code table*

Alarm type	Alarm type code
Urgent	1
Important	2
Commonly	3
Warning	4
Uncertain	5

Table 2. Alarm time segment coding table

Alarm period	Alarm time segment code
08:00-12:00	00
12:00-18:00	01
18:00-00:00	10
00:00-08:00	11

### 4.3. Mining Alarm Association Rules

The Apriori algorithm in this paper is used to mine the mining transaction table alarmtdata, and different rules are obtained by setting different support degrees and confidence degrees. The number of rules produced is shown in Table 3 below:

Table 3. Statistics of rule generation

Number of generation rules	Minimum Support (%)	Minimum Confidence (%)
1124	1	10
648	1	20
211	5	10
83	5	20
35	10	10
0	10	20

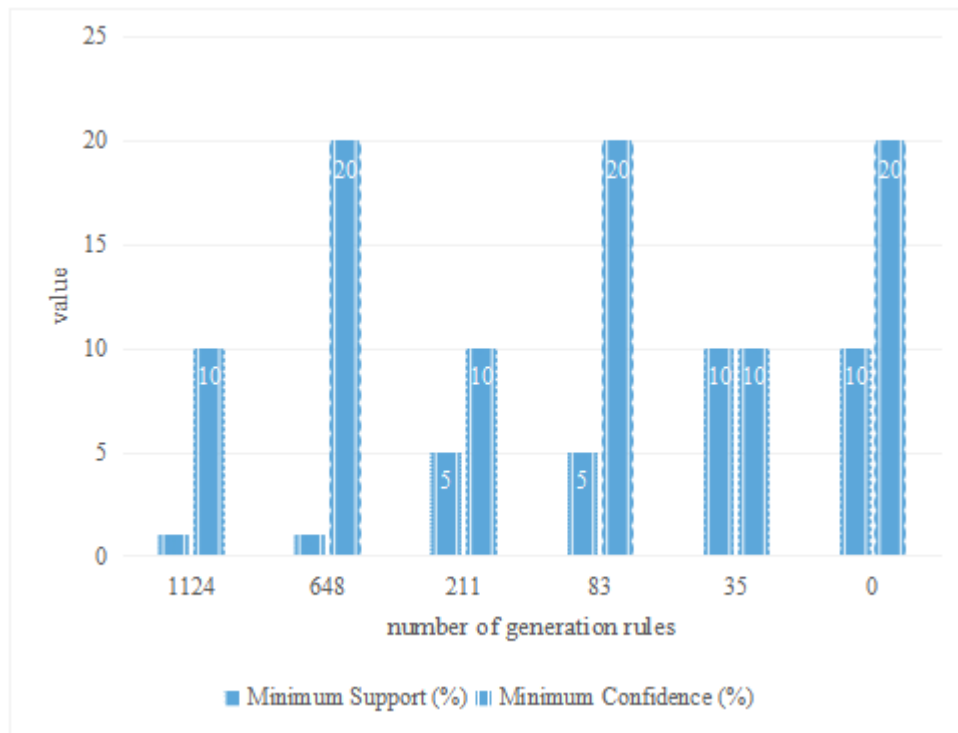


Figure 2. Alarm association rules mining results

As the support and confidence levels increase, the number of rules will become smaller and smaller, and the partial results with minimum support of 10% and minimum confidence of 10% are shown below, as shown in Figure 2.

Some of the rules are analyzed below. For the first rule :alarmptime=10  $\cap$  alarmcatalog=Unknown Person  $\Rightarrow$  alarmlevel=2(support=1.82%, confidence=66.8%). The meaning of this rule

is as follows: When the alarm time is between 6:00 PM and 00:00 am, and the alarm type is that an unknown person attempts to enter the alarm, the probability that the alarm is a major alarm is 66.8%. At the same time, the lifting degree of the rule is  $1.035 > 1$ , indicating that the two sides of the rule are positively correlated.

Maintenance personnel are interested in this rule. You can find out the alarm occurrence rule based on this rule. According to these rules, the maintenance staff can predict the alarm of campus access control.

At the same time for the rule: Alarm name = campus power failure  $\rightarrow$  Alarm level = critical (confidence=100%). This rule is obviously meaningless, because the alarm name outage alarm is an emergency alarm, this rule is not new.

## 5. Conclusion

Computer technology, network technology, the development makes the various universities has basically have send new campus security software and hardware environment needed for the entrance guard system, this system on the interface, humane treatment as far as possible, convenient operation, the use of this system for logistics information, analysis of students' safety can be effectively, The ability to mine association rules further increases the likelihood of finding useful rules. Due to time reasons, this system is not perfect; the function of each function module is still insufficient. In this system, only with the help of data mining association rules in the theory analysis, in the next stage, will further the research in the theory of data mining of other technology in campus security entrance guard system application value, so as to make the campus security entrance guard system in such aspects as policy auxiliary construction in universities, colleges and universities play a bigger role.

## Funding

This article is not supported by any foundation.

## Data Availability

Data sharing is not applicable to this article as no new data were created or analysed in this study.

## Conflict of Interest

The author states that this article has no conflict of interest.

## References

- [1] Tahir Ahmad, Umberto Morelli, Silvio Ranise, Nicola Zannone: *Extending access control in AWS IoT through event-driven functions: an experimental evaluation using a smart lock system. Int. J. Inf. Sec.* 21(2): 379-408 (2021) <https://doi.org/10.1007/s10207-021-00558-3>
- [2] Muhammad Tanveer, Abd Ullah Khan, Neeraj Kumar, Alamgir Naushad, Shehzad Ashraf Chaudhry: *A Robust Access Control Protocol for the Smart Grid Systems. IEEE Internet Things J.* 9(9): 6855-6865 (2021) <https://doi.org/10.1109/JIOT.2021.3113469>
- [3] Oladayo Olufemi Olakanmi, Kehinde Oluwasesan Odeyemi: *EACS: Expressible Access Control Scheme for Secure Services and Data Delegation in Collaborative E-health System. Inf. Secur. J. A Glob. Perspect.* 31(3): 274-288 (2021) <https://doi.org/10.1080/19393555.2021.1926603>

- [4] Shubham Devidas Gujar, S. Fouziya Sulthana, Rajesh Anbazhagan: Development of dual access energy monitoring for the smart control system. *J. Ambient Intell. Smart Environ.* 14(2): 119-133 (2021) <https://doi.org/10.3233/AIS-210356>
- [5] Otávio Seidi Nishimura, Jos é Carlos Marinello Filho, Taufik Abrão, Richard Demo Souza: Fairness in a Class Barring Power Control Random Access Protocol for Crowded XL-MIMO Systems. *IEEE Syst. J.* 16(3): 4574-4582 (2021) <https://doi.org/10.1109/JSYST.2021.3156696>
- [6] Sujit Biswas, Kashif Sharif, Fan Li, Iqbal Alam, Saraju P. Mohanty: DAAC: Digital Asset Access Control in a Unified Blockchain Based E-Health System. *IEEE Trans. Big Data* 8(5): 1273-1287 (2020) <https://doi.org/10.1109/TBDATA.2020.3037914>
- [7] Amit Kumar Sikder, Leonardo Babun, Z. Berkay Celik, Hidayet Aksu, Patrick D. McDaniel, Engin Kirda, A. Selcuk Uluagac: Who's Controlling My Device? Multi-User Multi-Device-Aware Access Control System for Shared Smart Home Environment. *ACM Trans. Internet Things* 3(4): 27:1-27:39 (2021) <https://doi.org/10.1145/3543513>
- [8] Padmavathi Iyer, Amirreza Masoumzadeh: Learning Relationship-Based Access Control Policies from Black-Box Systems. *ACM Trans. Priv. Secur.* 25(3): 22:1-22:36 (2021) <https://doi.org/10.1145/3517121>
- [9] Pratima Sharma, Rajni Jindal, Dutta Borah Malaya: Blockchain-based cloud storage system with CP-ABE-based access control and revocation process. *J. Supercomput.* 78(6): 7700-7728 (2021) <https://doi.org/10.1007/s11227-021-04179-4>
- [10] V. A. Tokareva: Schedules with Priorities for Online Resource Management Problems in Aggregated Data Access Systems. *Autom. Remote. Control.* 82(11): 1939-1948 (2021) <https://doi.org/10.1134/S0005117921110096>
- [11] Salim El Khediri, Adel Thaljaoui, Fayez Alfayez: A Novel Decision-Making Process for COVID-19 Fighting Based on Association Rules and Bayesian Methods. *Comput. J.* 65(9): 2360-2376 (2021) <https://doi.org/10.1093/comjnl/bxab071>
- [12] Trinh T. T. Tran, Tu N. Nguyen, Thuan T. Nguyen, Giang L. Nguyen, Chau N. Truong: A Fuzzy Association Rules Mining Algorithm with Fuzzy Partitioning Optimization for Intelligent Decision Systems. *Int. J. Fuzzy Syst.* 24(5): 2617-2630 (2021)
- [13] Syam Menon, Abhijeet Ghoshal, Sumit Sarkar: Modifying Transactional Databases to Hide Sensitive Association Rules. *Inf. Syst. Res.* 33(1): 152-178 (2021) <https://doi.org/10.1287/isre.2021.1033>
- [14] Sahana P. Shankar, Naresh E., Harshit Agrawal: Optimization of association rules using hybrid data mining technique. *Innov. Syst. Softw. Eng.* 18(2): 251-261 (2021) <https://doi.org/10.1007/s11334-021-00387-6>
- [15] Dede Rohidin, Noor Azah Samsudin, Mustafa Mat Deris: Association rules of fuzzy soft set based classification for text classification problem. *J. King Saud Univ. Comput. Inf. Sci.* 34(3): 801-812 (2020) <https://doi.org/10.1016/j.jksuci.2020.03.014>
- [16] Seyed Hassan Mirhashemi, Farhad Mirzaei: Using combined clustering algorithms and association rules for better management of the amount of water delivered to the irrigation network of Abyek Plain, Iran. *Neural Comput. Appl.* 34(5): 3875-3883 (2021) <https://doi.org/10.1007/s00521-021-06648-6>
- [17] Marina Vives-Mestres, Ron S. Kenett, Santiago Thi ó-Henestrosa, Josep-Antoni Mart ín-Fern ández: Measurement, selection, and visualization of association rules: A compositional data perspective. *Qual. Reliab. Eng. Int.* 38(3): 1327-1339 (2021) <https://doi.org/10.1002/qre.2910>
- [18] Mai Shawkat, Mahmoud Badawi, Sally M. El-Ghamrawy, Reham Arnous, Ali I. Eldesoky: An optimized FP-growth algorithm for discovery of association rules. *J. Supercomput.* 78(4): 5479-5506 (2021) <https://doi.org/10.1007/s11227-021-04066-y>