Analysis of the Relevant Characteristics of *Online Fraud Cases* Happened on College Students

Qiu Mingyue*, Wang Xinmeng, Zhao Mingsheng, Wu Yubao
School of Information Technology, Nanjing Forest Police College, Nanjing, China.

* Corresponding author. Email: qiumy@nfpc.edu.cn
Manuscript submitted January 12, 2021; accepted May 25, 2021.
doi: 10.17706/ijeeee.2021.11.4.133-141

Abstract: In the Internet era, the college student groups are Internet users who use the Internet more widely and deeply with more frequency than the ordinary Internet users. However, college students have insufficient social experience and they have been living in a relatively simple living environment for a long time, which makes them have low ability to distinguish the true from the false and become the targeted by cyber scammers easily. This paper analyzes the causes and the basic types of online fraud cases happened on college students through studying the current situation of online fraud cases happened on college students so as to guide college students to learn to screen and self-protect, and to cultivate more comprehensive high-quality talents.

Key words: The college student, online fraud cases, Apriori, correlation analysis.

1. Introduction

With the development of big data technology and Internet of Things technology, the forms of crime and the types of crime are also changing. The forms and the methods of online fraud are different from the traditional fraud. They make use of the Internet to target college students, a simple group, and acquire the information of college students through the emerging technologies so as to realize the purpose of precision fraud. College students are in their adolescence, who have a wide range of hobbies and a strong ability to accept new things. However, because of insufficient social experience of college students, as soon as the external information is in line with their own cognition as well as values, they will receive it as the right information, so it is easy for them to believe the words as well as guidance of others. College students have a wide range of hobbies and generally spend a lot of time online. In the meantime, they are curious about new things on the Internet, so they are not easy to be aware of some new types of fraud. They think they are an emerging Internet product or a business model innovation. Because of the regular online behaviours of college students and their weak awareness of prevention, their daily online information and a variety of personal information are easily obtained by others through illegal methods, thereby judging their identity, preferences, user habits, etc. The criminals make false fraud cases or even tricks specifically for college students, so that college students will be taken in, thereby obtaining illegal benefits. Thus, we should strengthen the anti-fraud publicity and education of college students, and conduct a variety of publicity when the freshmen first enter universities so as to achieve a comprehensive online anti-fraud education and to prevent college students from being easily deceived.

This paper studies the relevant characteristics of college fraud, fraud time, crime, and other methods,

providing data support and scientific basis for the relevant strategic measures to prevent college fraud cases, so as to reduce the probability of similar cases and maintain a good Network usage environment. The remainder of this paper is organized as follows. Section 2 describes the relevant research. Section 3 provides the statistical analysis of telecommunications fraud cases happened on college students. Then, we apply the Apriori association analysis in Section 4, and provides a discussion in Section 5.

2. The Relevant Research

Because of the rapid development of the Internet era, the traditional types of crimes have gradually changed into new types of network crimes, leading to the frequent cases of online fraud in recent years. A literature search on the topic of "Fraud on College Student" on HowNet found that the number of papers had remained at less than 5 papers per year until 2016. Until the "Xu Yuyu Case", the attention of the whole society has been aroused and the number of papers also has a great improvement. Many scholars have begun to explore the relevant characteristics and the influencing factors of online fraud cases happened on college students. For instance, Wang Fei and others have made an analysis on the current situation and prevention strategies of online fraud cases happened on college students in a big data environment, who focus on the distinguishing features and the reasons for being deceived of the contemporary college students, and the countermeasures for such cases [1]-[3]. Li Shanshan analyzed the characteristics of online fraud under the background of big data and the reasons why college students are subject to online fraud, who also analyzed the types of online fraud among college students and put forward some specific ideological and political education countermeasures [4]. There are also scholars who studied the relationship between fraud cases and victims. Li Xiaobing researched the association rules of fraud cases based on the Prior algorithm. It was found that the fraud time was at noon and the bank was located in a bank. The losses were relatively serious rules. [5]. Li Shuang designed a telecom fraud case recognition classifier on the basis of a convolutional neural network. Through the study of telecom user bill data, he mined the characteristics of call data of fraud users and identified the behavior of fraud users [6]-[8]. Thus, in this paper, the basic characteristics of telecommunications fraud cases happened on college students have been gradually changed into deep case mining, and the association rules of telecommunications fraud cases happened on college students have been further explored.

3. Statistical Analysis of Telecommunications Fraud Cases Happened on College Students

3.1. Time of the Case

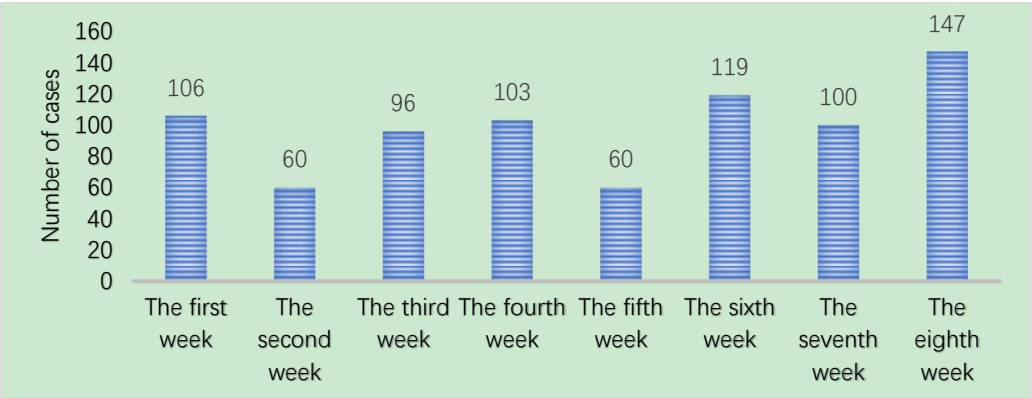

Fig. 1. Number of telecommunications fraud cases happened on college students per week after the school starts on September 1st.

With September 1st as the date when school begins, the analysis of the timing of the college student fraud cases were carried out weekly. It can be seen from Fig. 1 that there have been cases of college students' telecommunications fraud every week since the beginning of school, and the number of the cases has been relatively large. At the beginning of university, students usually bring their living costs, tuition fees and other expenses to start the semester. Thus, many criminals make use of behavioural characteristics such as weak awareness of college students, insufficient social experience and frequent Internet access to realize the purpose of accurate deception in a short period of time. In addition to the usual anti-fraud publicity and education work, schools and the relevant education departments shall strengthen the cyber security education of college students in the first two months of the school season, so that students can master the necessary fraud prevention measures and reduce or prevent the occurrence of telecommunications fraud among college students.

3.2. The Length of Crime

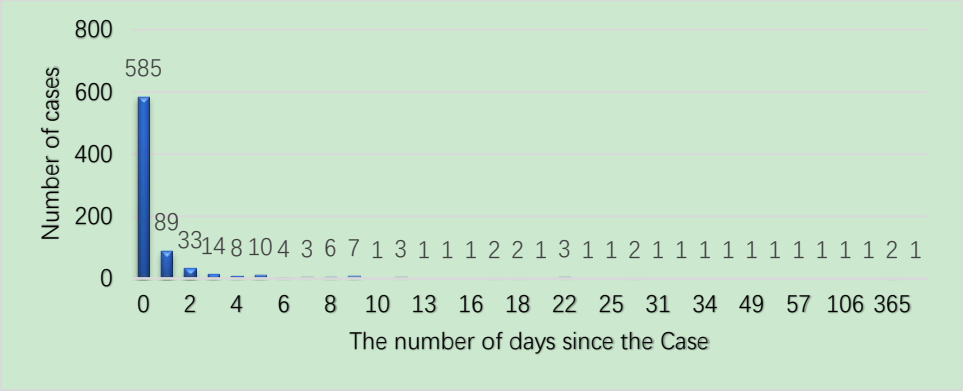

Fig. 2. Statistics on the number of days of telecommunications fraud cases happened on college students.

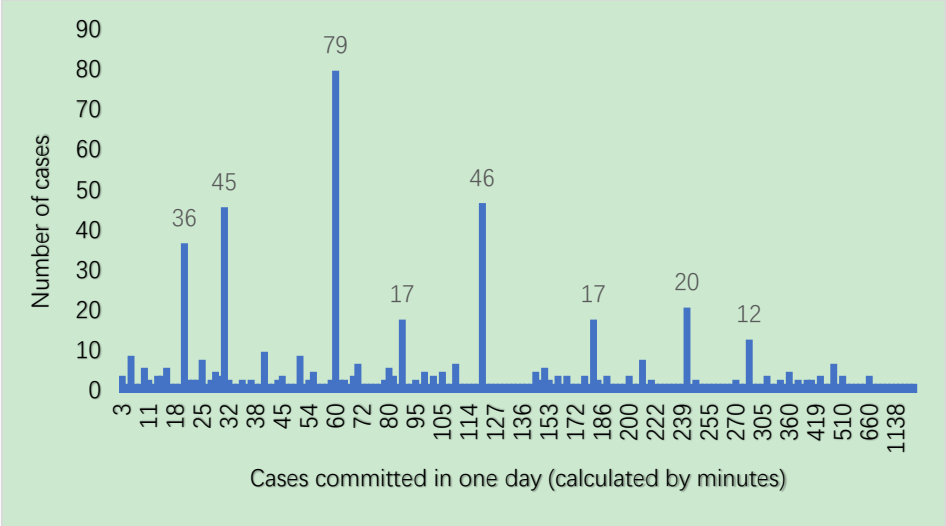

Fig. 3. Time statistics of telecommunication fraud cases (cases in one day) among college students.

In accordance with the comparison of the upper limit and lower limit of the time of the incident, it can be known that the average telecommunications fraud cases happened on college students occur within one day (as shown in Fig. 2). Among the cases that occurred within a day, the largest number of cases was 60 minutes, that is, the one-hour criminal suspect committed the most fraudulent acts against college student victims. Besides, the length of the fraud process is concentrated in 120 minutes, 30 minutes, and 20 minutes,

respectively. It can be seen from this that the incidence of telecommunications fraud cases happened on college students is very short. Once they enter the designed fraud trap, they will be taken in in a short time.

3.3. Reporting Time

The victims of telecommunications fraud will usually choose to call the police when they find that they have been deceived, but the analysis data show that not everyone will choose to ask the police for help as soon as possible. Compare the lower limit of the incident time with the reporting time, that is, the time interval between the time when the victims are designed to be deceived and then the time when they call the police immediately. The data shows that most people choose to promptly report within one day (as shown in Fig. 4, the probability is 77%), and the victims who report to the police within one week reach 96%. It can be known from the experience of police's handling cases that, in general, in the telecommunications fraud cases, the time within 1 hour after victim's money is transferred to the suspects' relevant account is the prime time to intercept the flow of funds. Thus, in the future publicity associated with telecommunications fraud, the effectiveness of publicizing the time of calling the police shall be strengthened to recover the economic losses of the victims as quickly as possible.

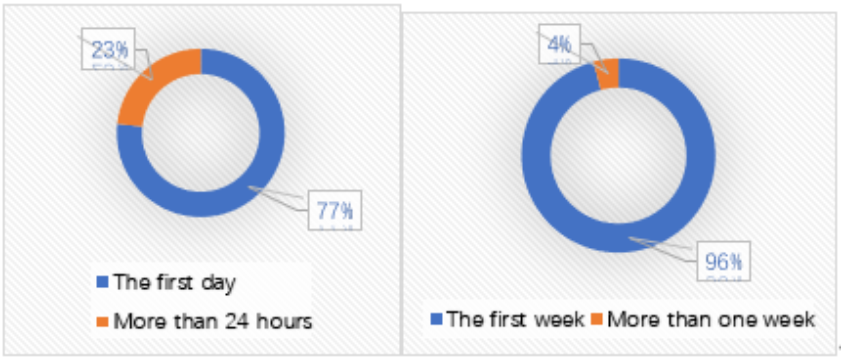

Fig. 4. Interval of calling the police in college students' telecommunications fraud cases.

By combining the analysis of the case data in September and October of 2014-2018, it can be found that the afternoon and the evening are the high-incidence duration of the cases. Among them, afternoon (14: 00-18: 00) accounts for 28%, and evening accounts for (18: 00-24: 00) accounts for 47%. This is also closely associated with the online schedule of college students. College students are generally accustomed to consulting information and entertainment on a computer from afternoon to evening, which is corresponding to the time when the cases happen. The time of calling the police by the college students in the case of telecommunications fraud happened on college students is also mostly concentrated in the afternoon and evening, as shown in Fig. 5.

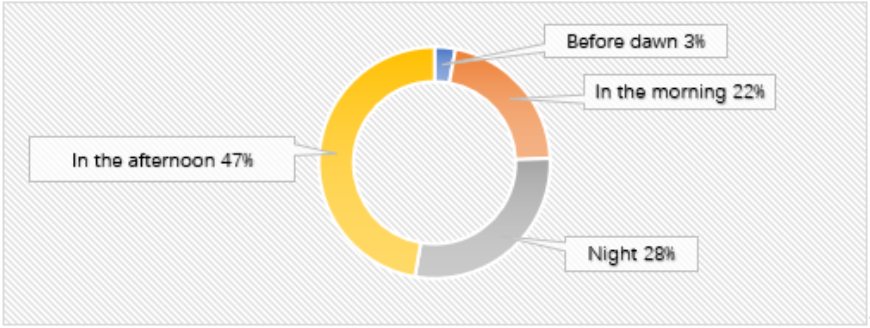

Fig. 5. Time of calling the police in a telecommunications fraud case happened on college students.

3.4. Fraud Amount

In accordance with the "2011 Interpretations of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues Concerning the Specific Application of Laws in Handling Criminal Cases of Fraud", the value of fraudulent public and private property valued at 3,000-10,000 yuan or more, 30,000-100,000 yuan or more, and 500,000 yuan or more shall be respectively identified as "relatively large amounts", "large amounts" and "especially large amounts" as stipulated in the 266th clause of the Criminal Law. Thus, the starting point for general online fraud crime cases is 3,000 yuan. If it is less than 3,000 yuan, the people will be punished in accordance with the relevant regulations. This paper classifies the amount of fraud in telecommunications fraud cases happened on college students on the basis of the above provisions. It can be seen from Fig. 6 that in the cases of telecommunications fraud of college students, the fraudulent amount reached 47%, and the proportion of fraudulent amounts of 3,000 to 30,000 yuan reached 48%. It can be seen that the number of small-scale fraud cases among telecommunications fraud cases happened on college students accounts for the vast majority, and the proportion of crimes with large amount and the especially amount is particularly large.

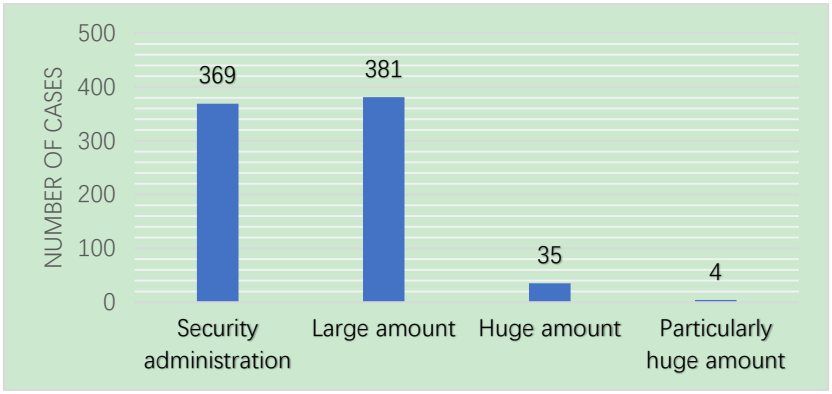

Fig. 6. Statistics on the losses amount of telecommunications fraud happened on college students.

3.5. Case Category

In the statistics of telecommunications fraud cases happened on college students, online fraud accounts for 77% of the total telecommunications fraud cases, telephone fraud accounts for 20%, and SMS fraud accounts for 3%. It can be seen that, because of college students' online habits and weak awareness of protection, online fraud has dominated the major classification of telecommunications fraud cases happened on college students. In the following paper, this paper also mainly analyzes the relevant factors and characteristics of online fraud cases happened on college students. In accordance with the analysis of online fraud cases, online shopping accounts for the largest proportion of fraud, reaching 44.3% of the total number of cases, which is also frequently associated with the online shopping behavior of college students. The second are bank card cases (15.06%) and impersonation of acquaintances (10.51%), which are mostly associated with college students' low awareness of self-defense and the fact that college students are easy to trust others. Among them, the method of pretending an acquaintance also occupies a certain proportion in phone frauds. Suspects usually claim to be government officers, school teachers, courier and other service personnel to defraud the victims into trust, and then ask the victims transfer funds to relevant accounts, thereby seeking illegal interests.

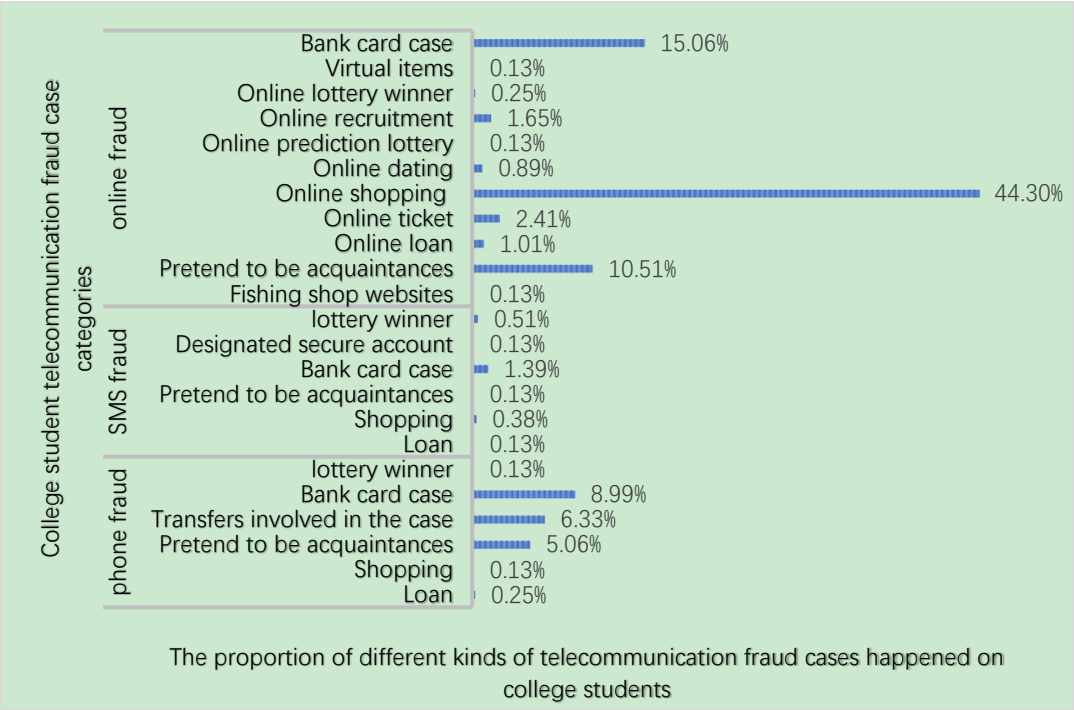

Fig. 7. Statistics on the proportion of different kinds of telecommunications fraud cases happened on college students.

4. Mining of Online Fraud Cases Happened on College Students Based on Apriori Association Analysis

4.1. Association Network Chart

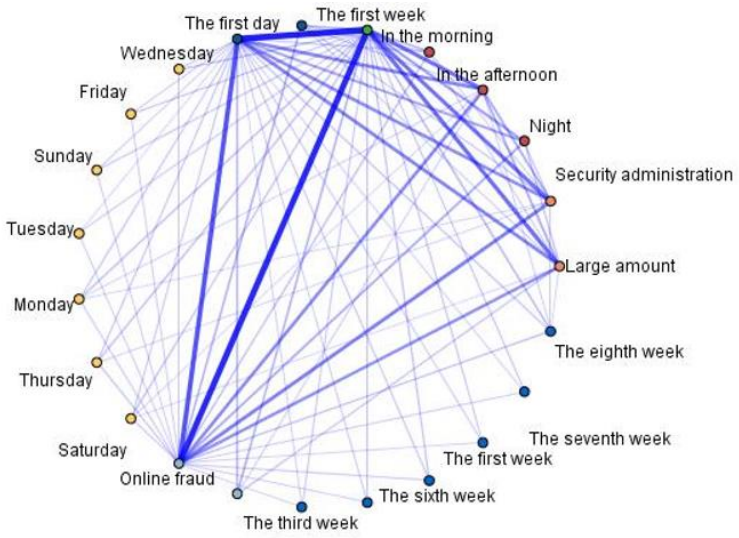

Fig. 8. Association network chart.

Through network chart which can show the strength of the correlation between categorical variables, this paper displays the relationship among categorical variables such as case category, reporting period, reporting time (day, week), penalty amount category, and weeks before / after school opens as shown in Figure 8. The lines in the figure reflects the frequency of the two variables, that is, the strength of the correlation. The relevant network chart can intuitively show that there is a strong correlation between

online fraud and the first week and day of reporting, and the amount of penalty in the case is relatively large. It shows that the victims of college students will choose to report to the police in time when they find that they have been deceived, and the amount of the majority of the cases of online fraud cases happened on college students are small frauds under 30,000 yuan.

4.2. Mining of Online Fraud Cases Happened on College Students on the Basis of Apriori Correlation Analysis

Table 1. Analysis of Online Fraud Cases Happened on College Students on the Basis of Apriori Association Analysis

Next item	Previous item	Support	Confidence
Case category = Online fraud	Reporting time=More than 24 hours Penalty amount category=Security penalty	11.378	91.111
Case category = Online fraud	Reporting time=More than 24 hours Reporting time period=Afternoon	10.24	87.654
Case category = Online fraud	Penalty amount category=Security penalty Reporting time period=Afternoon	22.882	85.635
Case category = Online fraud	Reporting time period=Evening Penalty amount category=Security penalty	12.769	85.149
Case category = Online fraud	Penalty amount category=Security penalty	46.776	85.135
Case category = Online fraud	Reporting time=More than 24 hours	23.262	84.783
Case category = Online fraud	Reporting time=Tuesday	12.01	83.158
Case category = Online fraud	Reporting time period=Morning Reporting time=More than 24 hours	10.114	82.5
Case category = Online fraud	Weeks before / after school opens =The seventh week	12.642	81.0
Case category = Online fraud	Week of reporting = Saturday	14.286	80.531
Case category = Online fraud	Reporting time period=Evening	28.319	80.357
Case category = Online fraud	Weeks before / after school opens = The eighth week	18.584	80.272

Association rules are an unsupervised data mining algorithm which finds the association between data through analyzing the data. In short, it is because of the occurrence of some events that other events occur. Apriori is one of the main algorithms of association rules. It belongs to an unsupervised learning method, which can reveal the underlying association features effectively in the data and reveal the internal structure of things.

From Table 1 and through Apriori correlation analysis, the rules are drawn as follows: when the time of calling the police is more than 24 hours after the case happens, and in accordance with legal provisions, it only constitutes a law and order violation and has not yet constituted a criminal crime, among the many fraud cases, the confidence coefficient of online fraud cases is highest, accounting for 91.111%. When the reporting time is more than 24 hours after the case happens and the reporting time period is in the afternoon, among many fraud cases, the confidence coefficient of online fraud cases is 87.654%, ranking the second. The above two highly relevant association rules together show that when the case is reported more than 24 hours after the incident and the amount of fraud is small, it doesn't yet constitute a crime. Or, when a fraud case occurs in the afternoon, it is usually an online fraud.

The victims in the online fraud cases happened on college students are usually more careless about the nature of online fraud in the small amount of public security cases ranging from 0 to 3000 yuan. College students generally hold the idea that small payments or loans will not have serious consequences on their own economy, and the small amounts of money are still within the acceptable range of daily life for college students. As a result, the victim group usually can't call the police in time after being deceived on the Internet. In general, they will not be aware of the fact that they have been deceived one day after the case, thereby calling the police. But because they have missed the prime time of calling for the police, this will cause some difficulties for the police's arrest. In the meantime, the period from afternoon to evening is the

high-incidence duration of such online fraud cases, which is associated with the mentality of daily class hours. In general, in the afternoon and evening, after college students finish their day of study, their awareness of precautions begins to decline, which makes it easier for criminal suspects to perform online fraud on college students.

5. Conclusion

Online frauds show a trend of diversification, precision and virus spread. As an active force of Internet users, college students lack enough social experience and rational thinking. We could provide techniques to prevent or recognize the online fraud for college students based on this study for future research. Thus, in the era of big data, we should make good use of big data technology to carry out an in-depth and comprehensive research on the status and characteristics of online fraud cases happened on college students. Healthier and comprehensive learning and growth, training high-quality modern talents.

Conflict of Interest

No conflict of interest exists in this research, and the manuscript is approved by all authors for publication. The authors declare that the work described was original research that has not been published previously, in whole or in part. All the authors have approved the manuscript that is enclosed.

Author Contributions

Qiu Mingyue contributed significantly to analysis and manuscript preparation; Qiu Mingyue performed the data analyses and wrote the manuscript; Wang Xinmeng performed the experiment; Zhao Mingsheng helped perform the analysis with constructive discussions; Wu Yubao contributed to the conception of the study.

Acknowledgment

This study is partially supported by Project No. : 2019131014, Research on Grassland Fire Risk Forecast and Early Warning Mechanism Based on Big Data, 2019 Soft Science Research Project of National Forestry and Grassland Administration；Project No. 2018LLYJSLGA021, “Research on Working Methods of Online Masses of Public Security Organs in the ‘Internet +’ Era”, Project on Ministry of Public Security Theory and Soft Science Research Plan; National first-class undergraduate major (network security and law enforcement) construction project.

References

[1] Wang, F., Wang, T., & Huang, S. (2018). The status quo and prevention strategies of college students’ internet fraud in the big data environment. *Legal Expo*, *02*, 41-43.

[2] Li, S. (2018). The status quo of college students’ internet fraud and the countermeasures of ideological and political education in the big data environment. *Knowledge Economy*, *24*, 168-169.

[3] Li, X. (2015). Research on mining association rules of online fraud cases on the basis of the apriori algorithm. *China Management Informationization*, *18(13)*, 219-222.

[4] Ji, H., Ma, Y., & Li, S. (2017). Feature recognition method of telecommunication fraud on the basis of SVM. *Software*, *38(12)*, 104-109.

[5] Rad, H. A., Arash, S., & Rahbar, F. (2015). A novel unsupervised classification method for customs fraud detection. *Indian Journal of Science and Technology*, *8*, 17-35.

[6] Iqbal, F., Fung, B. C., & Debbabi, M. (2019). Wordnet-based criminal networks mining for cybercrime investigation. *IEEE Access*, *7(22)*, 40-55.

[7] Gebru, M. M. (2018). Association pattern discovery of import export items in Ethiopia. *American Scientific Research Journal for Engineering, Technology, and Sciences*, *44(1)*, 40-56.

[8] Zehero, B. B., Soro, E., & Gondo, Y. (2018). Elicitation of association rules from information on customs offences on the basis of frequent motives. *Engineering*, *10(9)*, 588-605.

Qiu Mingyue works in Information Technology College of Nanjing Forest Police College, and the research direction is data mining. The author is mainly engaged in the research and teaching of data mining, big data, etc., and has accumulated a lot of knowledge and experience related to the theory of information science and data modeling. The author actively explores the development direction of information science in the era of big data and studies how to integrate advanced big data technology into the theoretical research and practical work of information science.

Wang Xinmeng works in Information Technology College of Nanjing Forest Police College, and the research direction is information technology. He has engaged in information technology-related research for many years and has accumulated a lot of information technology-related work experience.

Zhao Mingsheng works in Information Technology College of Nanjing Forest Police College, and the research direction is network information technology. He has engaged in network information technology-related research for many years and has accumulated a lot of information technology-related work experience.

Wu Yubao works in Information Technology College of Nanjing Forest Police College, and the research direction is network information technology. He has engaged in network information technology-related research for many years and has accumulated a lot of information technology-related work experience.