Hindawi
Journal of Robotics
Volume 2023, Article ID 9860830, 1 page
https://doi.org/10.1155/2023/9860830

Retraction

Retracted: Research on the Detection Countermeasures of Telecommunication Network Fraud Based on Big Data for Killing Pigs and Plates

Journal of Robotics

Received 19 September 2023; Accepted 19 September 2023; Published 20 September 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope
(2) Discrepancies in the description of the research reported
(3) Discrepancies between the availability of data and the research described
(4) Inappropriate citations
(5) Incoherent, meaningless and/or irrelevant content included in the article
(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] G. Li and Y. Wen, "Research on the Detection Countermeasures of Telecommunication Network Fraud Based on Big Data for Killing Pigs and Plates," *Journal of Robotics*, vol. 2022, Article ID 4761230, 11 pages, 2022.

Hindawi
Journal of Robotics
Volume 2022, Article ID 4761230, 11 pages
https://doi.org/10.1155/2022/4761230

Research Article

Research on the Detection Countermeasures of Telecommunication Network Fraud Based on Big Data for Killing Pigs and Plates

Gang Li[1] and Yong Wen[2]

[1]*Guangxi Police College, Nanning 530028, Guangxi, China*
[2]*School of Artificial Intelligence, Guangxi University for Nationalities, Nanning 530006, Guangxi, China*

Correspondence should be addressed to Yong Wen; 20190304001@stu.gxun.edu.cn

Received 2 December 2021; Revised 18 January 2022; Accepted 12 February 2022; Published 7 March 2022

Academic Editor: Shan Zhong

This paper uses big data analysis to conduct in-depth analysis and research on the investigation countermeasures of the pig-killing dish telecommunication network fraud. This paper takes the case of "piggy bank" as a perspective, starting from analyzing the concept and characteristics of "piggy bank" type network fraud, analyzing the current phenomenon of this type of network fraud crime, and analyzing the current situation of the relevant laws, to explore the judicial situation regarding this type of network fraud crime, and to explore the problems and dilemmas in the judicial determination of such network fraud crimes, the determination of evidence, the determination of principal and accessory in joint crimes, the determination of crime amount, the determination of attempt and attempt form, and the determination of related crimes. Based on the analysis of the problems, the judicial determination process of "piggyback" network fraud is improved in terms of perfecting the evidence determination process, combining the facts of the whole case to determine the joint crime, accurately characterizing the associated criminal acts, regulating the judicial determination rules of the crime amount, and strictly applying the criteria of the circumstances of attempt and completion. This paper explores the forward shift of investigation work, anticipating telecommunication network fraud crimes in advance or the middle of the matter through active investigation, taking technical countermeasures, especially early warning and dissuasion to avoid the occurrence of telecommunication network fraud crimes, and reversing the unfavorable situation of passive investigation in the past. Finally, it focuses on the strategy and innovation points of the use of network investigation methods in telecom fraud crimes and proposes the investigation method of tracing the money chain and information chain along the line and cross-complementing the two lines at the same time according to the characteristics contained in telecom fraud crimes, relying on multiple groups such as public security, hackers, and network volunteers to jointly combat in a variety of network environments.

1. Introduction

With the information technology revolution sweeping up, the digital economy is growing at a geometric rate, and science and technology have penetrated all human production life and social interaction, and people are not bound to the traditional face-to-face communication at all, but more often choose noncontact information exchange [1]. At the same time, following the development of communication and network media, telecommunication network fraud is rapidly spreading and expanding, not only infringing on the most basic economic interests of the people but also endangering the sustainable development of the economy and society, increasing the risk and difficulty of social management, and the governance of telecommunication network fraud, a hot issue of people's livelihood, is gradually highlighting its importance and urgency in the field of social management. How to effectively manage telecommunication network fraud has become a social issue that needs to be urgently addressed by government departments at all levels [2].

The first half of 2020 was affected by the epidemic and the economic downturn in all sectors. The pressure on employment increased, the epidemic made it impossible for people to leave their homes, and people shifted their productive lives to the Internet, making telecommunication network fraud crimes frequent [3]. While the Internet is enriching people's lives, Internet technology is also being used by criminals, which makes traditional contact crimes decline and noncontact crimes represented by telecommunication network fraud crimes occur frequently. Nowadays, telecommunication network fraud, as a highly prevalent crime, is also making renovations and changes in line with the development of society. "Impersonating public prosecutors and law enforcement officers" is the primary version of telecom network fraud. Criminals continue to upgrade the criminal techniques on this basis; "loan lending" has become an upgraded version of telecom network fraud [4]. When "lending" became the key target of public security authorities, criminals designed new fraudulent ways according to the new needs of society; thus the "piggy bank" telecom network fraud came into being. The "piggy bank" type network fraud refers to the perpetrator to "love" "dating" and other means to deceive the victim's trust, with a variety of reasons to induce the victim into the precontrolled false. The victim is then lured into gambling and investing on a false website or platform for various reasons and then cheats the victim out of money. Due to the rapid spread and continuous renovation of online and noncontact fraud, telecommunications network fraud is no longer just an illegal and criminal act but has become a hot spot of social concern and difficulty in governance. As an upgraded version of telecommunication network fraud, "piggy bank" is more concealed and more socially harmful. In recent years, the "piggy bank" type of network fraud cases has been a high trend and has become one of the main ways of committing telecommunication network fraud. However, because the crime is characterized by a variety of criminal acts, concealed criminal means, and a long-lasting crime, the effectiveness of the public security authorities in combating and preventing it is not obvious [5].

In such an environment, to effectively curb and prevent the continued high incidence of telecommunication network fraud cases, society has made more efforts to strengthen institutional supervision, enhance technical support, and optimize combat effectiveness. However, due to the rapid spread and continuous renovation of network-based and noncontact fraud forms, telecommunication network fraud is no longer just an illegal criminal act but has developed into a hot spot of social concern and a difficult point of governance [6]. There is still a large gap between the actual effectiveness of telecom network fraud governance and the current situation of crime, economic losses, and the expectations of the public. How to break the current predicament faced by governance from the perspective of actual combat is a topic worth studying.

2. Related Works

Internet fraud has been around since when the knowledge of contemporary telephone communication became widespread in the developed countries of the West, and with the advancement of telephone communication, frauds can be committed without the risk of "face-to-face contact," by impersonating identities over the telephone and setting up various frauds to make illegal profits [7]. The high incidence of such cases has led to serious damage to citizens' money, so most Western countries have actively engaged in research and study of this issue in the fight against Internet fraud. One of the effective ways they have adopted is to increase the management of the real-name system so that the privacy of each citizen can be protected to the maximum extent and at the same time, establish relevant databases to reduce the crime of Internet fraud at the source [8]. Not only that, but foreign countries have also made more specific elucidation around the legal punishment of network fraud. For example, the US federal law on such cases is specified, according to the actual amount of fraud to develop the corresponding sentences, to prevent the emergence of judicial corruption in the sentencing process. In addition, the FBI has also cracked down on cyber fraud, drawing on the relevant statistical reports of the US FCC, and has implemented monitoring and data analysis of ex-convicts in many countries and regions around the world and has created cyber fraud complaint centers, relying on huge data for comparison and analysis, so that criminals have nowhere to hide. It has also prepared severe legal penalties. In addition, severe legal penalties have been prepared to suppress fraudulent behavior [9]. The United States is the first and most advanced country in terms of network construction, and it has a wealth of practical experience in the management of cyber fraud, and many countries such as Japan have also actively borrowed from the United States in their legal management of cyber fraud.

The "mobile phone in the hand, the world I have" is a true picture of people's travel life, with a variety of clothing, food, housing, and transportation APP online, going out without a wallet with a mobile phone has become a habit of life for most people; increased suspects aim at this new direction, depending on the popularity of mobile payment and online shopping [10]. They impersonate online shopping platform customer service, to "after-sales service," "inferior recall," and other reasons, to lure the victim by remodifying the payment order and other methods to transfer the money in the bound bank card, which is the most typical crime of telecom fraud crime, one of the modus operandi. The investigation will always lag the crime, and from the practical side, as the modus operandi of telecom fraud crimes continues to be renovated, the number of its cases also continues to climb, but the detection rate is generally low [11]. At this stage, suspects use increasingly developed communication technology and fast payment means to create a variety of frauds to implement fraud in a noncontact state, and telecom fraud crime cases are still in a high incidence and low detection situation. The earliest academic research on network fraud should have originated in Taiwan when the research was conducted on the spread of network fraud cases from Taiwan to the mainland coast [12]. The continuous development of network technology has led to a high incidence of network fraud as well. By studying and finding the similarities between different incidents of cyber fraud crimes, many researchers aim to start with the theory and explore the underlying causes of the composition of this crime type and the ways to deal with it later, to propose strategies and recommendations to combat cyber fraud crimes [13].

3. Big Data-Based Model Designs for the Detection of Telecommunication Network Fraud in Piggy Banks

3.1. Building a Big Data Analytics Model. To deal with different cases of Internet fraud, government departments have continuously adjusted their governance programs, and public security authorities have gradually made improvements to their detection methods, grasping special remedies and making such cases a key target of their crackdown. The use of governance crackdowns across the country and extreme publicity has effectively curbed the spread of fraudulent activities [14]. The media, along with financial institutions in general, have used prominent signs to also inform the public about the various types of frauds and the dangers they pose to society. The coverage and publicity of telecom network fraud have substantially increased the public's awareness of prevention. However, each case is still a high-risk factor for cyber security. To solve and get out of the immediate dilemma of fraud, typical cases around the country need to be used as a vehicle to analyze the shortcomings and deficiencies of the country's public governance and bring reference to the relevant departments to improve the efficiency of governance. Reviewing the typical cases that have occurred around the country, we find that there are certain commonalities behind these online frauds. From the analysis of the above fraud cases, their modus operandi is all relatively close. The fraudsters all impersonate their identities and use a kind of virtual scenario to commit fraud. Although the education and identity of the victims were different, ranging from high school graduates to finance and accounting staff of famous enterprises to university graduates, they all came across frauds of a bad nature. In addition, two of the victims paid with their lives for this. From this, it is enough to recognize that frauds are very harmful to this society. This is since telecommunication network frauds are now pervasive and they will always find ways to find their targets.

$$\max h_{j0} = \frac{u_r y_{rjo}}{v_i x_{ijo}}. \tag{1}$$

The New Crown epidemic in the early part of the 20th century broke the routine of the entire society. "With the outbreak of New Crown pneumonia across the country and even the world, fraudsters took advantage of the global shortage of antiepidemic supplies to perpetrate a new wave of frauds, taking advantage of the nervous urgency to procure masks, alcohol, and other supplies. The fraud during the "New Pneumonia" epidemic is a fraud that is "tailored" to the uniqueness of the events taking place during a specific period [15]. It has its uniqueness compared to the frauds of normal life, and during this period, this fraud was significantly more numerous, significantly more successful, and significantly more socially dangerous. In terms of the main target, these fraud cases are becoming increasingly precise in terms of their implementation. Long before committing a crime, criminal groups have basic information about the victim from different sources, including occupation, finance, etc. The inadequacy of the personal information confidentiality system has allowed these fraudsters to find opportunities. From the follow-up review, most of the fraudsters use the Internet to collect the information of the victims and combine their identity and occupation to implement the fraud. In this regard, this paper designs a crime case analysis model based on the big data of previous telecommunication frauds, as detailed in Figure 1.

To effectively carry out the prevention and combating of telecommunication network fraud, the Ministry of Public Security has summarized and announced 48 common telecommunication network frauds to society. In practice, the Ministry of Public Security's platform for investigating telecom network fraud cases divides telecom network fraud into 19 categories and 53 subcategories. However, there are so many different types of frauds that the above figures cannot cover all types of telecom network frauds. In addition, under the vigorous crackdown by public security organs, criminals continue to renovate and upgrade their modus operandi, and many new types of frauds such as "piggy banks" appear and grow, and the types of telecommunication network frauds that are highly prevalent in different periods may vary. This paper intends to analyze the current high incidence of telecommunications network fraud types of modus operandi to solve the case to indicate the direction of the investigation and provides reference for targeted early warning, dissuasion, and accurate prevention. The "killing pig" type of online fraud means that after the perpetrator defrauds the victim's trust under the guise of "love" and "friendship," he induces the victim to gamble and invest in precontrolled fake websites and platforms for various reasons, and defraud the victim of money—a new type of cybercrime.

From the number of criminal cases of telecommunication network fraud in Texas in 2019, the top five cases were 718 brush-off frauds, 430 loan frauds, 342 investment and finance frauds, 162 refund frauds posing as shopping customer service, and 102 online dating induced gambling and investment frauds (kill pans). As shown in Figure 2, single-scaling scams topped the list.

From the 2019 Texas telecommunication network fraud cases loss amount, the loss occupying the top five is an investment and financial fraud 30,959,700 yuan, brush single type fraud 15,261,400 yuan, online dating induced gambling, investment fraud (kill the piggy bank) 12,986,800 yuan, loan fraud 9,357,200 yuan, and impersonating shopping customer service refund fraud 4,519,700 yuan. A comprehensive analysis of the above shows that the current high incidence of common types of telecommunication network fraud is swipe type fraud, loan type fraud, investment, and finance type fraud, online dating induced gambling, investment fraud (piggy bank), and impersonation of shopping customer service refund fraud.

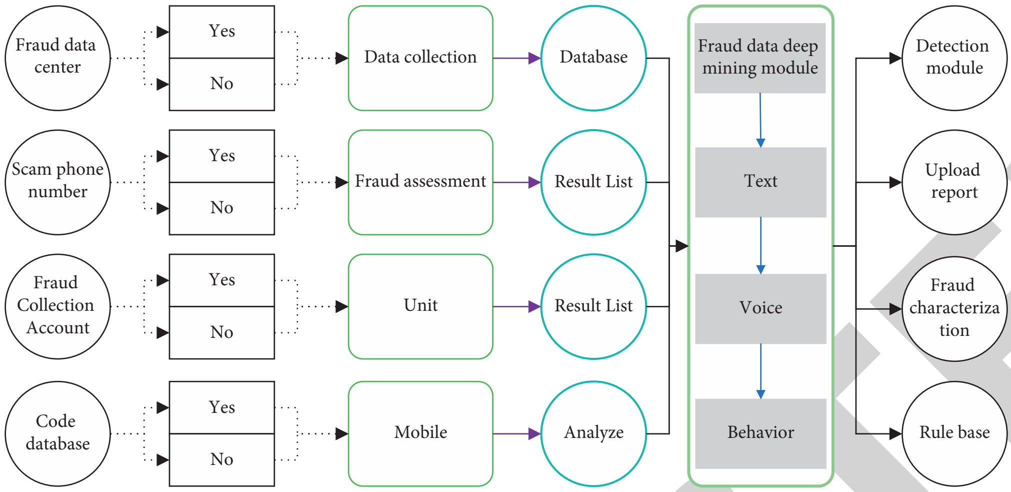

Figure 1: Flow chart of big data analysis of telecom fraud.

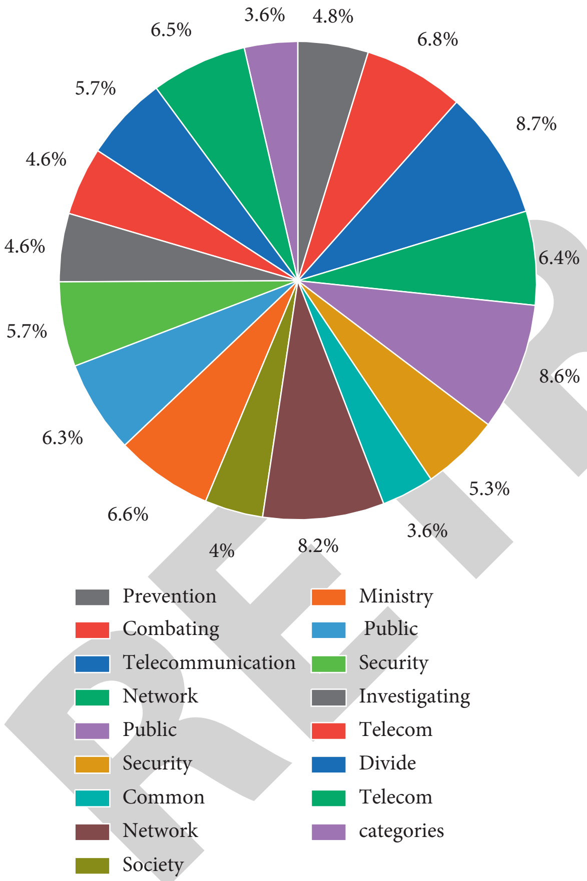

Figure 2: Statistical analysis of telecommunication network fraud cases.

$$\alpha = \frac{1}{v^t x_1^0},$$
$$\sum_{i=1}^{n} Y_{rj} - S_r^- = Y_{rj0}. \tag{2}$$

With the rapid development of the Internet, all kinds of e-commerce platforms, and rapid development and growth, online shopping is becoming increasingly popular and has gradually become an essential part of people's lives. When shopping online, the important reference for people to choose online stores is the sales volume and good reviews; some online, stores to improve sales volume and good reviews, they will hire "water army" to brush single; to enhance competitiveness, the "part-time job" of online brushing was born, many of which are professional white-collar workers and full-time earners with a certain amount of free time. The "part-time job" has emerged. Many have some free time; eager college students, professional white-collar workers, full-time mothers, etc., have joined the army of the brush single. At the same time, criminals also aimed at this opportunity, taking advantage of people being anxious to seek part-time jobs and greedy for cheap psychology, under the guise of recruiting network single personnel to implement fraud, brush single fraud has developed into the most frequent type of telecom network fraud crime.

$$X = 0.9 + 0.1 \frac{X_i}{X_{\max} + X_{\min}}. \tag{3}$$

The victims of this type of fraud not only lose money, but also their feelings are cheated, and some people even have the idea of living lightly after being cheated. The suspects use the fake identity information purchased to register on the dating sites such as Lily.com, Century Jayquan, Zhenai.com, or add the victims as friends through short video social platforms such as Jitterbug, Raptor, Stranger, and other instant messengers such as QQ, WeChat and other nearby people functions, disguise themselves, pretend to be rich and handsome, rich and beautiful, successful people and other identities, in the name of love and dating contact with the victims, through a period of interaction to determine the relationship between men and women [16]. The fact is that the actual person who is in the position to get a good deal more than just a few of these is a lot more than just a few of these. At the same time, the suspects will tamper with the data in the background, creating the illusion that the victim is making money through investment, deceiving the victim into using the website loophole to make money and then asking the victim to invest; once the victim falls for it, many people will take out all their funds to invest, or even go to borrow money or loans, with great losses.

With the convenience of express coordination and convenient mobile payment, online shopping has penetrated all aspects of people's lives, such as clothing, food, housing, and transportation. The suspects obtained the victim's online shopping or express information through illegal channels, posing as website customer service, saying that the quality of the victim's purchase has problems, can give the corresponding compensation, or posing as customer service, saying that the loss of express can give financial compensation, and then induce the victim to scan the QR code or click on the link to log into the so-called claims website, and wait until they get the victim's bank card account, password, mobile phone verification code, and other information; after the money will be transferred away, the victim's PayPal reputation points cannot be refunded for the reason of guiding the victim online loans, and induce the victim to transfer the loan to the designated account.

3.2. Analyzing Past Cases with the Help of a Big Data Model to Obtain the Characteristics of "Piggy Bank" Telecom Network Fraud. The characteristics of telecommunication fraud crime are determined by its attributes and development trends, which are summarized in this paper as the following five points.

3.2.1. Indirect Contact and Strong Anonymity. The biggest difference between telecom fraud, as one of the variants of fraud crimes, and traditional fraud crimes is that the suspect does not have direct contact with the victim, but indirect contact through telecommunication channels such as telephone, SMS, WeChat and VoIP, and the victim often does not have the suspect's identity information, nor does he or she meet with the suspect, making it difficult to confirm the identity. The economic downturn in all occupations, the increased employment pressure, and the epidemic have made people unable to go out, and people have transferred their production and life to the Internet, resulting in frequent telecom and network fraud crimes. This is the most significant feature of telecom fraud crimes, which is why telecom fraud is also known as remote, indirect contact fraud.

3.2.2. Gang Collaboration and Cross-Territory Operations. Telecom fraud crimes are mostly group fraud. From the origin of telecom fraud crimes, most frauds require multiple people to complete the fraud. The division of labor is clear and the grouping is fine in the process of fraud implementation. For example, fraud gangs posing as public security, prosecutors, and law are divided into script groups, online chat groups, talk groups, money laundering groups, withdrawal groups, etc. At the same time, telecommunications fraud crimes present ecological, familial, and geographical characteristics. A certain type of telecommunications fraud only exists in one place. The gang-like and family-style crimes have undoubtedly increased the difficulty and risk of hunting down the public security organs. It is difficult for the public security organs to wipe out a certain gang. This is also one of the direct reasons for the low detection rate of the current telecommunication fraud crime cases.

3.2.3. Low Starting Point, "A Book of Profit". The original wire fraud crime required little investment, and a mobile phone, a few mobile cards, and a good script were all that was needed to perpetrate a complete fraud. The "lucrative" nature of wire fraud has surpassed drug crimes, while the sentencing range is much lower than that of drug crimes, and the current penalties are not effective in deterring suspected wire fraud offenders.

3.2.4. Clear and Fine Division of Labor, High Degree of Organization of Criminal Gangs, and Strong Technology. Like the evolution of a virus, telecom fraud continues to evolve and change as the battle between good and evil continues, "progressing" with technological advances. While traditional telecom fraud only relied on phone calls, today's telecom fraud can rely on high-tech equipment such as cat pooling devices (sending and receiving mass SMS messages), SMS sniffing devices (forcing the collection of signals to create fake base stations), GOIP devices (hiding real numbers), and high-tech systems such as group control systems (one person controlling multiple mobile phone terminals), and Trojan horse theft systems [17]. The public has never even heard of these devices and systems, which directly leads to the fact that such frauds cannot be prevented and many times, they are cheated without realizing it. In telecom network fraud crimes, the suspects work alone rarely, and most of them work in the form of gangs with obvious professional characteristics. The internal organization of the gang is tight and the division of labor is clear, mainly divided into organizers, material dealers, car dealers, technical service groups, telephone and promotion groups, money laundering groups ("water room"), withdrawal groups ("riders"); each group is closely coordinated, but also independent of each other. To avoid crackdowns, some gangs adopt enterprise-based management, formulate strict rules and regulations, and require the separate use of crime cell phones and life cell phones, with the criminal chain becoming more and more elaborate. The organizational structure of a complete criminal gang is rough as follows (Figure 3).

3.2.5. Broad Victim Base. Criminal gangs will not only target a specific region or be limited to certain specific people but are based on fraud dens, using mobile phone group calling systems and SMS groupers to implement fraud on multiple people at the same time, with a large and scattered number of victims across the country. Regardless of gender, age, education, or work, any mobile phone or Internet user may be a potential victim of telecommunication network fraud

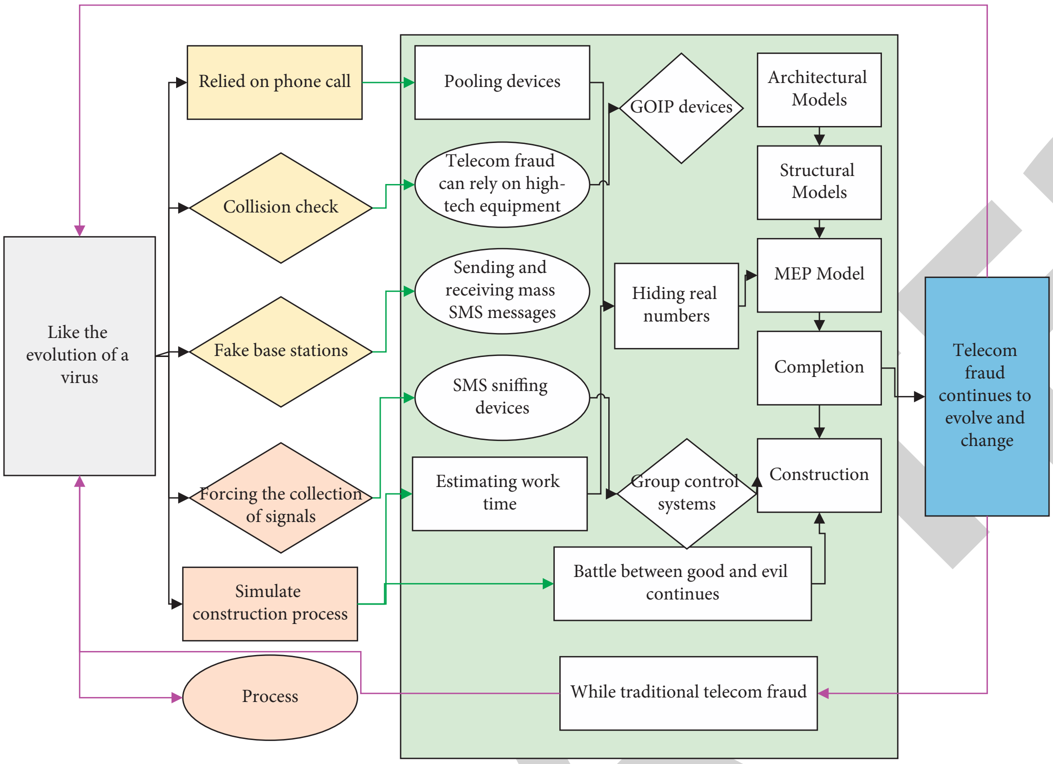
Relied on phone call
Collision check
Fake base stations
Forcing the collection of signals
Simulate construction process
Like the evolution of a virus
Process
Pooling devices
Telecom fraud can rely on high-tech equipment
Sending and receiving mass SMS messages
SMS sniffing devices
Estimating work time
GOIP devices
Hiding real numbers
Group control systems
Battle between good and evil continues
While traditional telecom fraud
Architectural Models
Structural Models
MEP Model
Completion
Construction
Telecom fraud continues to evolve and change

Figure 3: Organizational chart of the criminal group.

crimes. The base of mobile phone and Internet users in China is huge. As of June 2019, the scale of China's Internet users reached 854 million, the Internet penetration rate reached 61.2%, and the scale of online shopping users reached 639 million, accounting for 74.8% of the overall Internet users. Faced with a wide variety of fraudulent information, people are highly likely to fall into the trap of fraudsters and suffer property losses if they cannot accurately identify them.

$$R_p = \frac{N}{Q_{PL}}. \tag{4}$$

The high-tech features of telecom fraud crimes are currently reflected in the proficiency and use of sophisticated means of communication and electronic technology, and the suspects are more sophisticatedly equipped. Not only that, their knowledge base of psychology and other skills are also increasing, and the suspects are constantly updating their existing scripts by reading, analyzing, and deducing the possible psychological changes of their victims, and even marking even the tone aids and punctuation marks in their communication, which is amazing [18]. Due to the inconsistent level of access and proficiency in relevant information between the two parties to the transaction, where the dominant party may have more information, or exclusive and blocked information, while the disadvantaged party lacks sufficient necessary information, resulting in a situation where it is unable to make a full and effective decision, resulting in adverse consequences. In the prevention of bank telecommunication network fraud, banks are less autonomous in accepting government supervision for their interests, and the information available to the relevant regulatory authorities is not comprehensive enough to understand and confirm whether the corresponding regulatory policy requirements are implemented and put in place by banks, thus making it more difficult to assess the effectiveness of the relevant role of regulatory measures after implementation.

The leakage of citizens' personal information is serious due to the inadequate risk control measures of enterprises and institutions, lax internal supervision, and citizens' lack of awareness of information protection. Criminal gangs obtain victims' personal information through a variety of illegal means such as implanting Trojan horses, phishing websites, hacking, and black-market purchases, and then classify and develop different types of fraudulent scripts to implement precise frauds. In the types of frauds such as impersonating public prosecutors, impersonating customer service refunds, subsidized tax refunds, ticket changes, impersonating triads, etc., when the criminals accurately say the victim's name, ID number, home address, shopping orders, express delivery numbers, records of buying houses and cars, airline ticket orders and other information, some victims will relax their vigilance, reduce their ability to recognize, and are extremely vulnerable to being cheated.

Unlike other crimes, telecommunication network fraud requires the cooperation of the victim to be completed. To get the victim's cooperation, the suspect will prepare the script carefully in advance, master the fraudulent words, and take advantage of people's tendency to avoid harm, adopt bullying, and to lure the victim into believing their fabricated lies, and once the victim fails to recognize the fraud, he will fall into the trap and transfer money as requested by the suspect or provide his bank card number, password, verification code, and other information to the other party. In addition, anyone has cognitive limitations; some victims lack basic legal knowledge and unfamiliarity with relevant national policies, airline ticket change process, shopping platform claims, etc., and do not understand the online loan process and the procedures required, resulting in serious information asymmetry between the victim and the suspect, resulting in the victim easily believing the suspect's fictitious identity and fictitious facts. The possibility of being cheated is extremely high. In recent years, to enhance people's awareness of prevention and prevention ability, the relevant functional departments have been committed to fraud prevention publicity, but there are still problems such as single form, uniform content, insufficient coverage, and poor targeting, which cannot arouse the interest of the propagandized persons; there are blind spots for publicity; even though a lot of human, material, and financial resources have been invested, they cannot achieve the expected effect, coupled with the blind self-confidence of some victims. Even if they receive fraud prevention publicity, they do not pay attention to it.

$$Q = \sum_{i=1}^{n} LB_i. \qquad (5)$$

4. Analysis of Results

4.1. Big Data Analytics Model Test Results. "Due to the popularity of online shopping and online payment, transaction fraud is the most prevalent type of fraud." The report also points out that consumers are becoming increasingly rational, in the face of "gifts" such as "pie in the sky" frauds; vigilance has increased significantl; pure profit frauds have decreased significantly, which is inseparable from the long-term unremitting publicity and guidance and targeted special treatment. Data show that the proportion of victims between the ages of 18 and 28 is as high as 54%, and the post-90s group has the highest probability of being cheated [19]. In this regard, the report analyzes that young people who are studying or have just entered society are prone to become the target of fraudulent techniques such as payment rebates, free shipping, low-cost lures, and part-time recruitment. Young people who have some work experience and a certain economic base have a higher proportion of frauds in pornography, online dating, and financial credit. For middle-aged and elderly people, the report points out that the amount of fraud is often higher, with the per capita number of victims over 45 years old being about 7,000 yuan, far more than other age groups. They are easily exploited and controlled when they encounter frauds about financial investment, health care, and network technology and invest large sums of money, which is also more difficult to persuade. The age distribution of victims of different fraud types is shown in Figure 4.

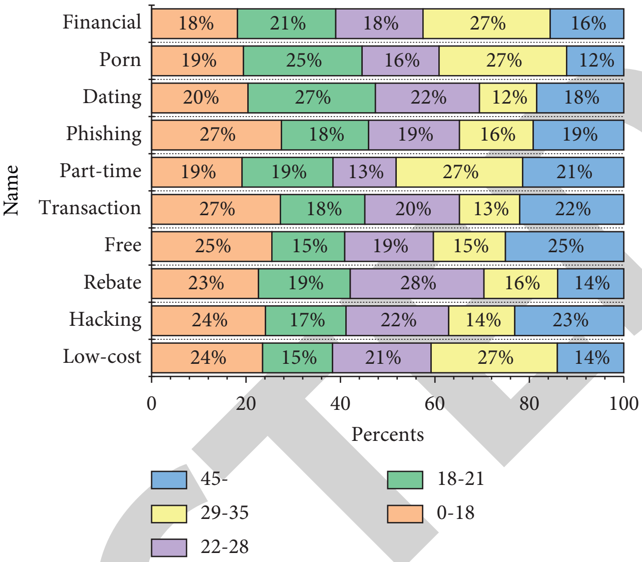

Figure 4: Distribution of age groups of victims of different fraud types in the last four years in County X.

Fraud brings great harm and has a wide impact, especially the use of telecommunications networks to engage in illegal and criminal activities that are highly concealed; so, in the specific implementation process, it is necessary not only to strengthen the fight but also to do a good job of prevention, to achieve comprehensive governance. Governance units include banking institutions, payment organizations, the Internet, and so on, in addition to relevant government departments. But in the specific governance process, there is an obvious phenomenon of division, especially when part of the work belongs to the crossover of the functions of multiple departments, it is easy to produce gray management, there is no lead unit, and some work is not covered or paid attention to, resulting in a regulatory vacuum. With the rapid change of science and technology, following the development trend of communication and network media, the rapid spread and expansion of telecommunication and network fraud has not only infringed the most basic economic interests of the people, but also endangered the sustainable development of the economy and society. At present, there are 25 departments in X County that deal with telecommunications network fraud. The units are more accustomed to independently undertaking their affairs. In the process of forming a joint effort, they are unable to achieve systematic unity for various reasons, such as distribution of interests, monopolization of resources, and competition for technical cores, etc. They are more based on interests and only undertake various tasks within the division of labor and pursue the maximization of departmental interests.

The manner of telecommunication network fraud has evolved with the changing times, and the scale of the syndicate, its technical means, and its concealment and confusion have expanded and progressed with the development of science and technology. The government's concept of governing telecom network fraud has not yet formed a relatively mature model, and the means and methods of combating, preventing, and controlling telecom network fraud lag significantly relative to the changes in such behavior. For the ever-changing forms of telecom network fraud entrapment, the full chain of crimes, cross-regional cross-border operations, and in information exclusion, fund interception, money destination, and propaganda prevention, all show a certain sense of powerlessness; the lawless elements in the front of the run, government departments in the back of the chase, and even the emergence of governance while flooding, this side of the governance of the situation over the flooding, the timeliness of the governance of illegal criminal behavior has also been discounted, invariably expanding the damaged side of the public [20]. In recent years, in the governance of illegal criminal activities arising from network telecommunications, the relevant government departments have invested a lot of resources and exerted much effort in terms of facilities and financial resources; in the establishment and operation of systems, mechanisms, and institutions, the industry has put a lot of effort, made a lot of attempts and practice. Still, from the actual governance effect, the spread of telecommunications network fraud has not been fundamentally transformed every day. There are still a large number of such policies and cases occurring, and the property security of the public is violated and damaged all the time. This phenomenon is widespread throughout the country. In terms of cost-benefit, the benefits and effects achieved by governance are far less than the costs and efforts invested, and a great deal of effort has been spent, but a good result has not been achieved, not to mention enhancing the public's sense of security and satisfaction. As shown in Figure 5, the fraud gang used a virus to implant electronic devices to obtain the suspect's personal privacy information, such as identity information, mobile phone number, payment password, bank card account password, etc.

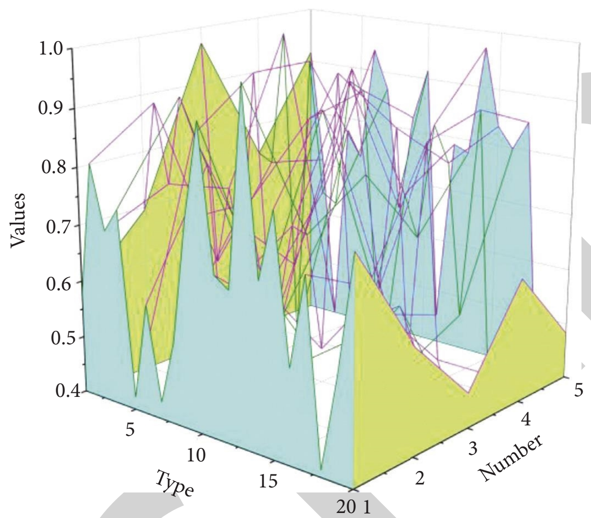

Figure 5: Distribution of telecommunications fraud viruses in household electronic products.

4.2. *"Pig-Killing Tray" Telecom Network Fraud Detection Simulation Test.*

In the judicial practice of pig killing plate network fraud crime, because this kind of fraud crime involves very complicated personnel, evidence, resulting in the public security organs investigation process, is more difficult because it is a network fraud, so most of the evidence involved is electronic evidence; in the process of crime, because the criminal facts occurred or the place of the criminal act is not accurate, it will lead to evidence that can be easily hidden or destroyed, thus increasing the resistance of the judiciary to evidence and factual determination. In the investigation of network fraud crime, the integrity and validity of evidence must be protected; to strictly punish the crime, accurate determination of the facts of the case must be ensured to achieve fairness and justice and to ensure the probative power of evidence. Access to electronic evidence to identify the network fraud crime is a very important link. Complete and effective electronic evidence for the conviction and sentencing of the crime is vital to accurately identify the behavior of criminals, fraudulent means and sentencing circumstances, accurate and standardized application of the law. In the investigation process, to ensure the effectiveness and integrity of electronic evidence, the investigating authorities in the collection and preservation of electronic evidence must be carried out in strict accordance with legal procedures and standardized means of investigation. This paper takes X city as an example to start a quarterly simulation test. A quarter of antitelecom fraud data statistics are as follows (Figure 6).

In the investigation process of the case, to do step-by-step division of labor, not a cluster, in the collection, preservation of electronic evidence involved in the case should be assigned to the public security organs special technical personnel to implement following the relevant legal provisions of lawful forensics, both to protect the integrity of the evidence and to improve the efficiency of the evidence acquisition process. Secondly, network fraud technology is becoming more and more novel, and the means are becoming more and more difficult to figure out; just like the pig-killing dish network fraud crime, criminals in the name of dating network fraud, the use of Internet technology to manipulate the software backstage, and criminal gangs work together, with a clear division of labor; in the process of combating crime to the forensic process of legality, effectiveness, the public security organs must improve the forensic, investigative capabilities. In addition, other network fraud crimes also exist using pseudobase stations, Trojan horse links, and other ways to obtain the victim's information, to use the victim's information to operate to obtain a large amount of property. With the derivation of intelligent crime tools, the suspect can use any number-changing software to fictitious facts to carry out fraudulent behavior. It is also due to the continuous updating of high-tech means of crime, resulting in more and more people being unsuspecting. It is also due to the continuous updating of high-tech modus operandi that more and more people are falling for the scam without any precaution, and the cases are frequent. In response to this situation, the government's means must also keep pace with the times, with the help of big data analysis model (as shown in Figure 7), after a quarter of the public security organs have significantly improved technical means, "kill plate" telecom network fraud has been significantly curbed.

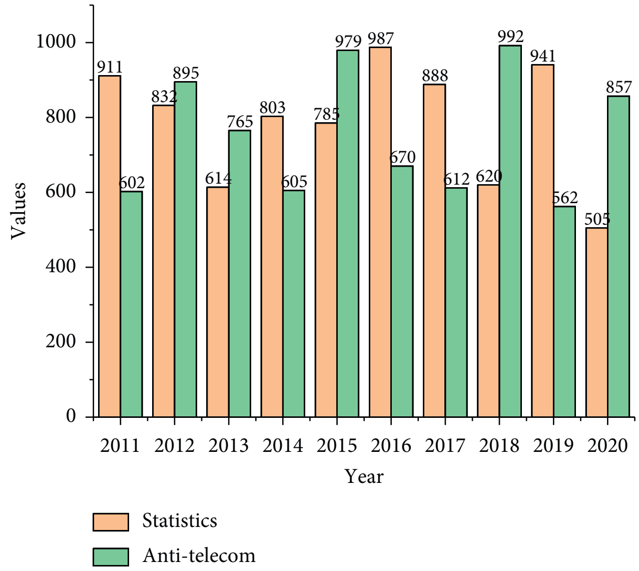

Figure 6: Q1 antitelco fraud big data report.

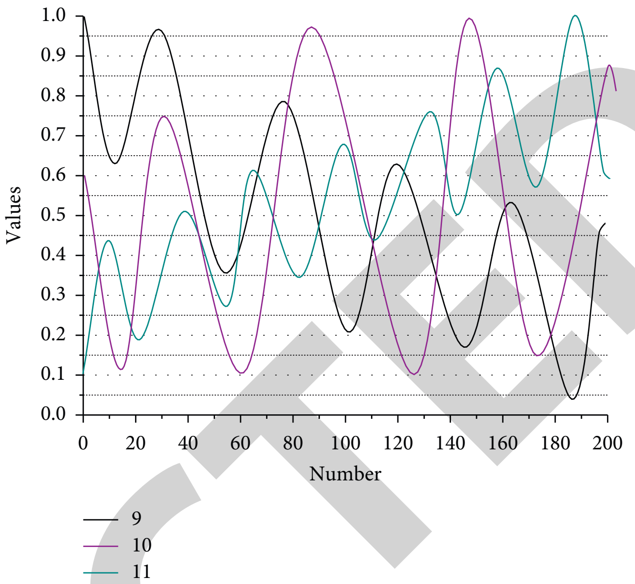

Figure 7: The decline of "piggy bank" telecom network fraud data in the first quarter of X city.

Strengthening regulation of the industries involved in telecommunications network fraud cases is an important means of improving governance capacity. Banks and telecommunications departments must implement the "real-name system" in strict accordance with the regulations and eliminate the existence of false, impostor, and shell bank cards and real-name card users. They should strengthen the cleanup of "black cards" and take effective measures to effectively solve the problem of "real names but not real people" on mobile phone cards, especially for new businesses such as Internet cards and Internet of Things cards, and carry out comprehensive risk assessments to prevent them from becoming tools for criminals to commit crimes. Banks and other financial departments should standardize the process of opening bank accounts, strengthen the audit and supervision of personal accounts and public accounts, judge the risk of fraud for unreasonable behavior that exceeds the set target, and observe the flow of funds and bank card account transactions to provide a basis for decision-making in the next step. Relevant functional departments should change the work system process, further limit the number of personal bank cards and telephone cards, clarify the legal responsibilities of individuals and units, and incorporate the real-name system of the telecommunications and financial sectors into personal social credit for the management, to solve the problem of unrealistic real names.

Telecommunications network fraud involves multiple sectors and aspects of society, not a matter for public security alone, the length of its illegal and criminal chain, the complexity and mobility of the people involved, must rely on the strength of all parties, and pool their efforts to govern. As the author, we should also actively contribute our part in the academic library, based on previous data, to give active literature research for society and public security organs, banks, and other relevant departments to borrow to study. From the statistics in Figure 8, the literature on "telecommunication network fraud" was published: the total number of articles was small in 2014, reached the peak in 2017, slightly decreased in 2018, warmed up in 2019, and always maintained a high degree of heat in recent years.

One of the important aspects of the governance of telecommunications network fraud is the game and confrontation between the scientific and technological capabilities of government departments and the renovation methods of lawless elements; only by continuously strengthening their technical countermeasure capabilities can they more efficiently research and detect lawbreakers and timely stop the implementation of interrupted telecommunications network frauds. What changes have taken place in the communication methods between people?

With the revolution of information technology swept up, the digital economy is growing at a geometric rate, and science and technology have penetrated all human production, life, and social communication methods. We must vigorously implement the protective technical measures of the Internet, telecommunications, financial, and other network enterprises to trace the perpetrators of telecom network fraud in the first instance and provide timely and effective assistance to public security departments in the process of apprehending suspects. Banks should further enhance the standard requirements for smart machine identification to avoid the impersonation of head cards through face recognition. Public security authorities, as the main department, to crack down telecom network fraud, have to strengthen team building to improve the business quality capabilities of public security authorities, which is the core of improving the effectiveness of combating telecom network fraud. Telecommunication network fraud seizes the psychology that the masses are greedy for small bargains, weak-minded and afraid of trouble, etc. Once the masses improve their self-defense ability, there will be no opportunity for fraudsters to take advantage of it. Therefore, it is

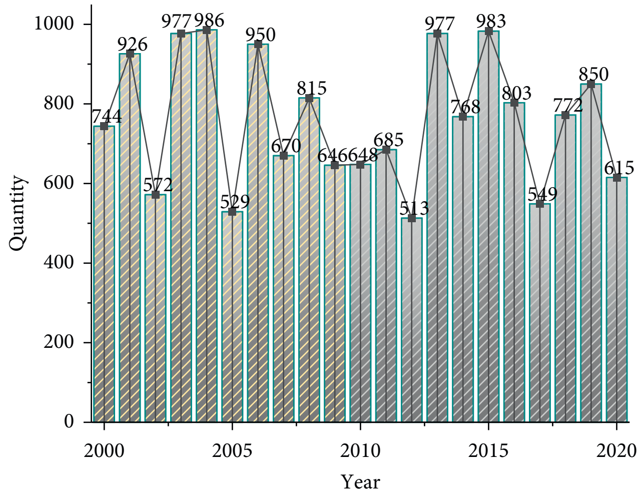

Figure 8: Annual trends in the publication of literature on “telecommunications network fraud”.

necessary to constantly carry out publicity work on telecommunication network fraud to citizens so that the public’s awareness of safety and prevention can be enhanced.

5. Conclusion

With the development of the Internet, telecommunications network fraud is frequent, and “piggybacking” as a new type of telecommunications network fraud crime, on the one hand, brings trauma to people’s emotions, and on the other hand, also makes people’s property suffer huge losses. The new era of network crime means constantly iterative updates; timely curbing the trend of network crime is imperative; public security organs should update the concept and implement diversified, multisectoral coordination of social security governance. At present, the effectiveness of the public security organs in combating “piggy-backing” network fraud is not obvious, which urgently requires an updated concept. In the era of big data, public security organs should address the characteristics of “piggy-back” telecom network fraud, expand intelligence sources, integrate and analyze intelligence information, strengthen the interconnection and mutual sharing of information resources, improve the investigative cooperation mechanism, establish a data-oriented prevention and early warning mechanism, and at the same time, pay attention to strengthening the protection of citizens’ personal information when retrieving clues. At the same time, attention is paid to strengthening the protection of citizens’ personal information when investigating clues, establishing a long-term mechanism for investigation, achieving “fast, accurate and fierce” combat against telecommunication network fraud crimes, protecting citizens’ property, and maintaining social stability.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This paper was supported by the Project Research and Practice on Teaching Reform of Public Security Based on Mobile Network Security Information Platform, supported by special project of 2019 Guangxi higher education undergraduate teaching reform foundation. Project Number: 2019JGB402.

References

[1] V. Jain, “Perspective analysis of telecommunication fraud detection using data stream analytics and neural network classification based data mining,” *International Journal of Information Technology*, vol. 9, no. 3, pp. 303–310, 2017.

[2] X. Liu and X. G. Wang, “Probabilistic graphical model based approach for bank telecommunication fraud detection,” *Computer Science*, vol. 45, no. 7, pp. 122–128, 2018.

[3] A. H. Ahmad, R. Masri, and C. M. Zeh, “The impact of digitalization on occupational fraud opportunity in telecommunication industry: a strategic review,” *PalArch’s Journal of Archaeology of Egypt/Egyptology*, vol. 17, no. 9, pp. 1308–1326, 2020.

[4] H. H. Kilinc, “A case study on fraudulent user behaviors in the telecommunication network,” *Electrica*, vol. 21, no. 1, pp. 74–84, 2021.

[5] H. Lin, G. Liu, and J. Wu, “Fraud detection in dynamic interaction network,” *IEEE Transactions on Knowledge and Data Engineering*, vol. 32, no. 10, pp. 1936–1950, 2019.

[6] G. Praveen, V. Chamola, V. Hassija, and N. Kumar, “Blockchain for 5G: a prelude to future telecommunication,” *IEEE Network*, vol. 34, no. 6, pp. 106–113, 2020.

[7] N. Zhang and Y. Xu, “Environmental study on cooperation system of cross-border tracking economic crimes based on block chain—take telecommunication fraud as an example,” *Ekoloji*, vol. 28, no. 107, pp. 4437–4446, 2019.

[8] M. Qiu and Y. Yang, “Analysis of the current situation and characteristics of college student “online fraud cases”,” *International Journal of Mobile Computing and Multimedia Communications*, vol. 12, no. 2, pp. 56–73, 2021.

[9] A. Battal and R. Samli, “An action management system design and case study on its usage for cyber fraud prevention and risk analysis,” *Journal of Innovative Science and Engineering*, vol. 5, no. 2, pp. 143–161, 2021.

[10] N. Duha, “Short message services (SMS) fraud against mobile telephone provider consumer review from law number 8 of 1999 concerning consumer protection,” *Journal of Law Science*, vol. 3, no. 1, pp. 36–43, 2021.

[11] N. Kala, “A study on internet bypass fraud: national security threat,” *Forensic Research and Criminology International Journal*, vol. 7, no. 1, pp. 31–35, 2019.

[12] R. A. Leite, T. Gschwandtner, S. Miksch, E. Gstrein, and J. Kuntner, “Visual analytics for event detection: Focusing on fraud,” *Visual Informatics*, vol. 2, no. 4, pp. 198–212, 2018.

[13] O. S. Yee, S. Sagadevan, and N. H. A. H. Malim, “Credit card fraud detection using machine learning as data mining technique,” *Journal of Telecommunication, Electronic and*

Computer Engineering (JTEC), vol. 10, no. 1-4, pp. 23–27, 2018.

[14] R. Zhu, H. Ye, H. Sun, X. Li, Y. Duan, and J. Hou, “Construction and application of knowledge-base in telecom fraud domain,” *International Journal of Intelligent Information and Database Systems*, vol. 14, no. 2, pp. 198–214, 2021.

[15] M. N. M. Mca, “Social network analytics (SNA) fraud,” *International Journal of Pure and Applied Mathematics*, vol. 118, no. 20, pp. 191–202, 2018.

[16] E. Jeong and J. Lim, “Study on intelligence (AI) detection model about telecommunication finance fraud accident[J],” *Journal of the Korea Institute of Information Security & Cryptology*, vol. 29, no. 1, pp. 149–164, 2019.

[17] Xinran, “China in their hands: the social credit system in China risks creating an all-controlling society where young people will, like generations before them, live in fear,” *Index on Censorship*, vol. 48, no. 2, pp. 74–76, 2019.

[18] K. U. Priya and S. Pushpa, “A survey on fraud analytics using predictive model in insurance claims,” *International Journal of Pure and Applied Mathematics*, vol. 114, no. 7, pp. 755–767, 2017.

[19] D. Baltimore, R. A. Charo, and D. J. Kevles, “Summit on human gene editing,” *National Academies of Sciences*, vol. 32, no. 3, pp. 61–69, 2016.

[20] G. Y. Koi-Akrofi, J. Koi-Akrofi, and D. A. Odai, “Global telecommunications fraud trend analysis,” *International Journal of Innovation and Applied Studies*, vol. 25, no. 3, pp. 940–947, 2019.