INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN BUSINESS & SOCIAL SCIENCES

Vol 14, Issue 3, (2024) E-ISSN: 2222-6990

Algorithm for the Legal Regulation of Internet Financial Crime

[1]Mao Xinxin, [2]Hanna Binti Ambaras Khan, [3]Suhaimi Bin Ab Rahman

[1]School of Business and Economics, Universiti Putra Malaysia, Jalan Universiti 1, 43400, Serdang, Selangor, Malaysia, [2]Senior Lecturer, School of Business and Economics, Universiti Putra Malaysia, Jalan Universiti 1, 43400, Serdang, Selangor, Malaysia, [3]Professor Dr., School of Business and Economics, Universiti Putra Malaysia, Jalan Universiti 1, 43400, Serdang, Selangor, Malaysia

Email: hanna@upm.edu.my, suhaimiabrahman@upm.edu.my

Corresponding Author Email: gs64631@student.upm.edu.my

To Link this Article: http://dx.doi.org/10.6007/IJARBSS/v14-i3/21130 DOI:10.6007/IJARBSS/v14-i3/21130

Published Date: 18 March 2024

Abstract

The study on the legal regulation of Internet financial crime holds significant importance in the context of the rapid development of China's Internet finance and the increasing prevalence of crime in this sector. To prevent crime, attention towards effective control of Internet finance crime has grown, emphasizing the protection of consumers' rights, reduction of economic damage, and promotion of Internet finance development. Data processing for criminal acts on Internet finance platforms is crucial, with the utilization of random forest algorithms, including Decision tree and Bagging integration algorithms. The methodology employed in this study is quantitative, focusing on the analysis of Internet financial crime using random forest and association rules based on data processing. The experiment results about the random forest in this paper showed that when the test sample was 600, the actual crime rate and the random forest prediction crime rate were 75.9% and 76.3%, respectively, and when the experimental sample was 600, the actual crime rate and the random forest prediction crime rate were 85.9% and 87.3%, respectively. The experiment results about association rules in this paper showed that with a sample size of 600, the correlation between the test sample and the experimental sample was observed to be 0.92 and 0.97, respectively. The experimental results indicated that the random forest algorithm demonstrated effective prediction abilities, with actual crime rates closely matching the predicted rates in both test and experimental samples. Similarly, association rules showed a strong correlation between the test and experimental samples, further validating the predictive capabilities of the algorithms. The findings underscore the effectiveness of random forest and association rules in predicting Internet financial crime, emphasizing the potential of computer algorithm combinations in crime prediction. The study highlights the importance of applying these algorithms to the legal regulation of Internet financial crime. Further research is proposed to delve deeper into the application of these algorithms in real-world scenarios and explore additional methods to enhance the prevention and management of Internet financial crime.

Keywords: Internet Financial Crime, Legal Regulation, Internet of Things, Random Forest, Data Processing

Introduction

Financial activities are the core of market economic activities in modern society. Despite the fact that Internet finance provides new channels for private finance and small and medium-sized financial institutions, the existing laws and regulations protect traditional finance to a greater extent. As a result, the laws and regulations governing Internet finance may be imperfect, giving criminals the opportunity to take advantage of them, resulting in a series of serious Internet financial crime. This has seriously violated the existing Internet order and ecology and the legitimate rights and interests of the country. Internet finance is a derivative of traditional finance. Internet financial crime in China has a significant damage impact on the financial market's stability. Therefore, in order to truly establish a sound and orderly order of Internet finance and safeguard the legitimate interests of all parties, it is necessary to scientifically analyze and sort out the legal regulations of Internet finance, and improve them in an all-round way, so as to effectively prevent and manage them in law. As user behavior data in the network has characteristics of complexity, large dimensions, large amounts of data, and so on, how to properly use, store, and filter variables is a pressing issue in Internet finance today. Using the intelligent environment of the Internet of Things to analyze the connection between all Internet financial crime is a significant economic and practical development.

In the current era of fostering the innovation of Internet finance, it is crucial to acknowledge the risks associated with this sector. Internet finance has, to some extent, facilitated the functioning of traditional financial industries while also amplifying systemic risks within the financial market. The key to regulating the development of Internet finance lies in implementing legal measures, guiding the industry towards orderly and compliant growth, and clearly defining the boundaries of applicable financial crimes. Acts that violate administrative regulations and severely disrupt market order should be subject to criminal punishment provisions.

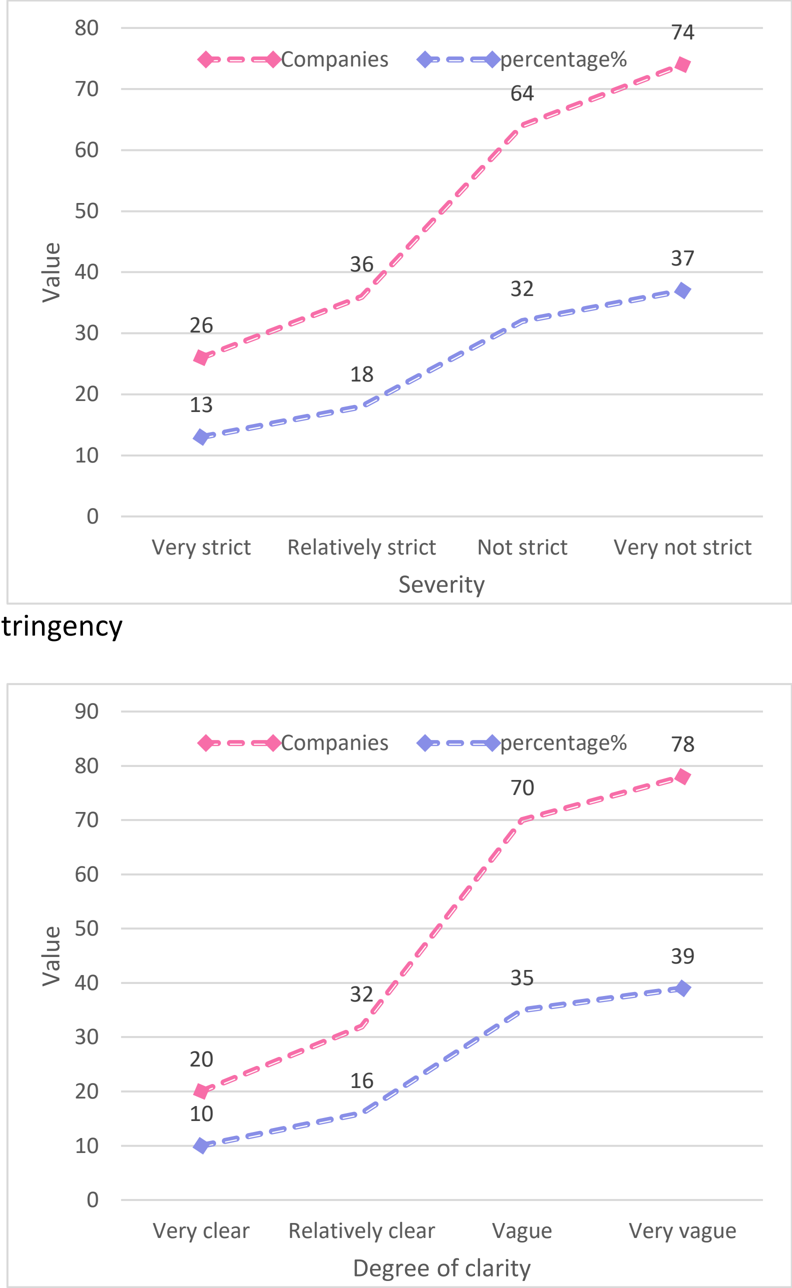
Analyzing and discussing the current situation, characteristics and new trends of Internet financial crime in China, paying closer attention to the changing trends of Internet financial crime, and discussing its prevention and control countermeasures are all for the purpose of better researching on preventing and combating Internet financial crime, to maintain normal economic and financial order, reduce economic losses caused by financial crimes, avoid financial risks, ensure a good financial environment, and escort the steady progress of a new round of financial reform in China.

Current Situation of Legal Regulation of Internet Finance Crime

With the advent of the Internet, the growth rate of Internet finance has reached unprecedented and unpredictable levels, exerting a profound impact on people's lives and work. However, like any tool, the Internet is a double-edged sword. While the development of Internet finance has brought unprecedented convenience, it has also given rise to some negative consequences. In an effort to assess the existing status of legal regulation pertaining to Internet financial crime and propose appropriate measures, this study conducted an investigation of 200 Internet financial companies located within a specific city through the Internet.

1) Inadequate supervision and ambiguous regulatory subjects

Internet finance business operations, regulations, and industry norms within Internet finance are not clearly defined, resulting in a regulatory gap. Internet finance represents a mix of high-risk financial activities on the Internet, encompassing risks inherent in both domains. The proliferation of risks, leading to potential concentration, hinders the establishment of an effective network financial supervision system. Insufficient regulatory stringency contributes to rapid risk accumulation, which hinders sustainable development. Figure 1 illustrates regulatory strictness and clarity:



(a) Regulatory stringency

(b) Regulatory clarity

Figure 1. Regulatory strictness and clarity

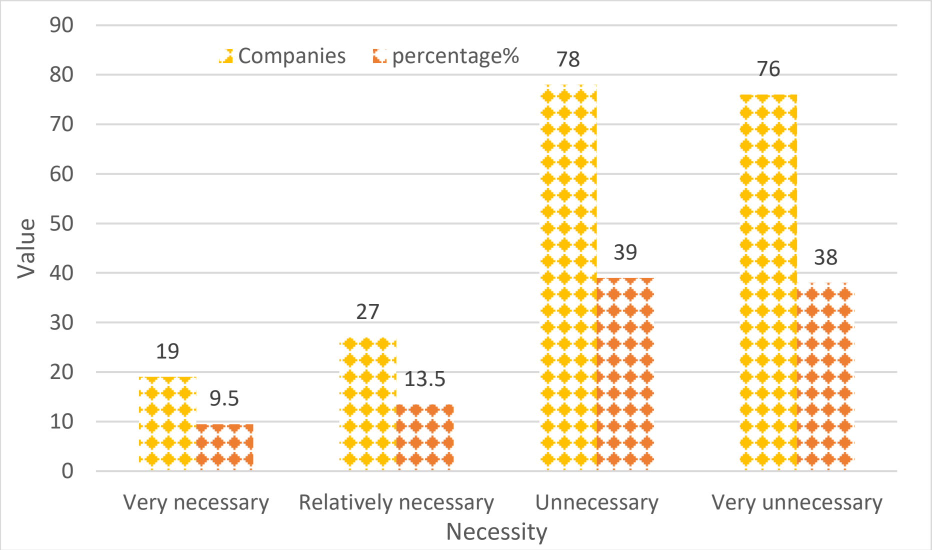
As depicted in Figure 1 (a), the findings reveal that 26 companies, representing 13%, perceive the regulation of Internet finance as being very strict, while 36 companies, accounting for 18%, consider it relatively restrictive. On the other hand, 64 companies, comprising 32%, believe that the regulation is not strict, and 74 companies, amounting to 37%, perceive it as very lax.

Moreover, Figure 1 (b) shows that 20 companies, accounting for 10%, believe that Internet finance regulation is very clear, and 32 companies, representing 16%, consider it relatively clear. Conversely, 70 companies, comprising 35%, find the regulations unclear, and 78 companies, amounting to 39%, believe the regulations are very unclear.

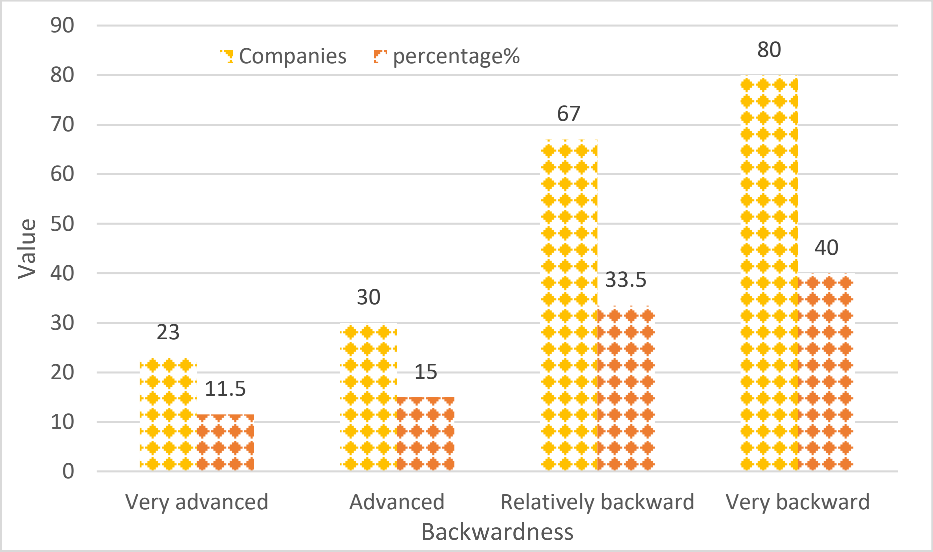
Internet finance represents the convergence of traditional finance and the Internet world. However, both financial supervision and Internet regulation face inherent challenges, resulting in an imbalance wherein financial supervision takes precedence. Consequently, this situation provides an opportunity for non-compliant actors to exploit the system, leading to a disruption in market order.

2) Backward technology

Many cyber-financial criminals take advantage of some website loopholes without encryption and security measures to maliciously tamper with normal websites, causing consumers to suffer fraud. It should attract the attention of financial website operators and managers, and strengthen the protection of their network security. Figure 2 shows the necessity of establishing information technology (IT) and its backwardness:



(a) Necessity of establishing IT



(b) Backward degree of IT

Figure 2. Necessity of establishing IT and backwardness of IT

Based on the observations presented in Figure 2 (a), it is found that 19 companies think it is very necessary to establish IT to prevent Internet finance crimes, accounting for 9.5%, and 27 companies think it is relatively necessary to establish IT, accounting for 13.5%. 78 companies believed that it was unnecessary to establish IT, accounting for 39%, and 76 companies believed that it was very unnecessary to establish IT, accounting for 38%.

Furthermore, Figure 2 (b) reveals that 80 companies, accounting for 40%, who feel that the IT for preventing cyber-financial crime is very backward, and 67 companies, accounting for 33.5%, who feel that the IT is relatively backward. There are 30 companies that think IT is advanced, accounting for 15%, and 23 companies that think IT is very advanced, accounting for 11.5%.

Information technology holds tremendous potential and offers robust operability. By leveraging techniques such as data recovery and encryption, law enforcement can significantly enhance their ability to detect and combat Internet financial crimes, amplifying their effectiveness in combating this growing threat.

3) Weak awareness of prevention

Confronted with the rise of cyber-financial crimes, numerous companies display a lack of preventive awareness, leading to the persistent occurrence of illicit activities and subsequently causing direct economic losses to both themselves and society at large. Companies often fail to prioritize information security and neglect adopting preventive measures prior to an incident, making it easier for cybercriminals to infiltrate their systems. Likewise, some consumers inadvertently overlook their own information security, casually disclosing personal information and accessing illegitimate websites. Table 1 showcases the preventive awareness levels among 200 companies:

Table 1
200 companies' awareness of prevention

Weakness	Number of companies	Percentage
Very weak	83	41.5%
Relatively weak	63	31.5%
Generally weak	33	16.5%
Strong	12	6%
Very strong	9	4.5%

As depicted in Table 1, a significant portion of companies, specifically 83 of them, demonstrate very weak awareness of financial crime prevention, accounting for 41.5% of the total. Another 63 companies, equivalent to 31.5%, exhibit relatively weak prevention awareness. Additionally, 33 companies, comprising 16.5%, have a weak prevention awareness, while 12 companies, representing 6%, possess strong awareness. Notably, nine companies display a strong level of prevention awareness, accounting for 4.5%.

Negligent practices such as accessing risky websites, indiscriminately opening unfamiliar emails, and overlooking the importance of network security firewalls expose companies to significant risks. Moreover, individuals must exercise sound judgment when encountering suspicious messages, such as requests for transfers or notifications of lottery winnings. Maintaining a high level of vigilance is crucial, as criminals often exploit low guard as a key enabler of their illicit activities. All relevant departments should actively promote awareness regarding Internet financial security to empower individuals to remain attentive to the diverse risks associated with online transactions and maintain a clear mindset.

4) It is difficult to crack down on Internet finance crime

The law represents a potent instrument, serving as a concentrated manifestation of state authority. However, the existing laws and regulations in China pertaining to Internet financial crime exhibit certain deficiencies, giving rise to challenges in judicial practice. Issues such as jurisdictional complications, which may impede timely case filing and consequently miss the optimal window for resolution, are prevalent. Additionally, the digital nature of criminal evidence, which is primarily electronic in form, poses significant challenges in terms of retrieval. In order to effectively address these challenges within the realm of judicial practice, an in-depth study is essential. Table 2 illustrates the complexities associated with combating Internet financial crime:

Table 2
Difficulties in combating Internet finance crimes

Difficulty	Number of companies	Percentage
Very large	79	39.5%
Relatively large	71	35.5%
Generally	28	14.0%
Small	16	8%
No	6	3%

As illustrated in Table 2, the task of combating Internet finance crime is widely regarded as highly challenging by 79 companies, accounting for 39.5% of the total. In contrast, 71 companies, representing 35.5%, consider it relatively difficult. Additionally, 28 companies, comprising 14.0%, perceive it as a difficult endeavor. Furthermore, 16 companies believe cracking down on Internet finance crime is challenging, constituting 8% of the total. Six companies opine that it is not difficult, making up 3% of the total.

Virtual networks empower criminals to transcend time and space. This catches victims off guard, enabling them to swiftly execute various criminal activities employing network technologies. From a legal standpoint, the current legislation in China exhibits gaps in access mechanisms, information security, and financial consumer protection. In addition, it exhibits deficiencies in relevant laws and regulations. The field of Internet finance entails significant risks, with various financial crimes conducted through online platforms characterized by substantial levels of concealment, complexity, and detrimental impacts.

Review of Literature

In recent years, there has been rapid growth in Internet finance in China, resulting in a large workforce and garnering significant attention across various sectors of society. Jelle (2021) emphasized the emergence of new opportunities for Internet finance crime due to the development of the Internet. Brands (2021) conducted a large-scale investigation and found that the general public's apprehension about Internet financial crime was moderate. The study also revealed that various socio-demographic characteristics and victim experiences can be used to predict Internet financial crime. Another study conducted by Fabian (2021) aimed to explore the use of cryptocurrency as a tool for financial crime. The findings highlighted the need for establishing international standards for blockchain and cryptocurrency regulations to effectively combat financial crimes associated with cryptocurrency. Moreover, practitioners should consider transnational cooperation in prosecuting such crimes (Teichmann et al., 2021). Additionally, Wronka (2022) noted the significant impact of the COVID-19 epidemic on various sectors of the global economy, including Internet finance crime. Wronka (2022) focused on the dual objectives of financial crime and investigated how financial institutions worldwide responded to and managed this emerging model of financial crime. Against the backdrop of the rapidly developing social economy, network fraud has shown an upward trend, making it one of the most pressing concerns in Internet crimes.

Internet financial crime has reached alarming levels, posing a threat to the ecosystem of Internet finance. A study conducted by Abdullah et al (2019) gathered data from financial crime cases involving Internet companies. The survey findings revealed a significant link between the presence of independent risk committees and incidents of financial crime. The empirical evidence from this impact study serves as a valuable indicator (Abdullah, Wan, & Roshima, 2019). Yang (2018) observed significant advancements in Internet finance in China. However, Yang (2018) pointed out that there are still legal gaps that need to be addressed. To effectively regulate Internet financial activities, supervision should align with market dynamics, employing mechanisms such as information systems and big data to reduce fraudulent information and financial crimes. It is crucial to ensure market transparency, competition, and fairness. Amjad and Rabia (2022) identified money laundering as a significant component of transnational financial crimes. Being well-planned and disguised, these crimes are challenging to detect and prevent. Their research aimed to examine the impact of globalization on financial crimes, particularly in the context of money laundering (Amjad and Rabia, 2022). In a word, the scholars emphasized that while the Internet has brought enormous development to the financial sector, it has also created numerous opportunities for Internet financial crime.

Characteristics of Internet Financial Crime

Liu (2022) thought that Internet finance brings numerous benefits to traditional financial institutions, allowing them to establish and strengthen customer management information systems. This enables quantitative management and informed decision-making. Furthermore, it enhances capital utilization efficiency within financial institutions and elevates their overall service capabilities. Internet finance offers comprehensive and interdisciplinary services, expands the service channels of financial institutions, and reduces operational costs. Presently, traditional financial institutions in many countries are actively embracing Internet finance, utilizing network technology to enhance pre-loan audits and post-loan supervision. Practical applications include crowdfunding, Internet microcredit, and others, but these advancements also raise the risk of Internet financial crime (Liu, 2022). Figure 3 illustrates the different types of Internet finance.

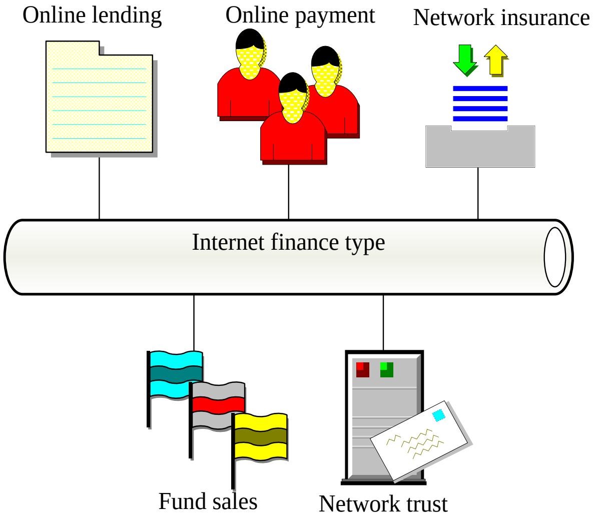


Figure 3. Types of Internet finance

As depicted in Figure 3, Internet finance encompasses various types such as Internet lending, Internet payment, Internet insurance, fund sales, and Internet trust (Liu, 2022). Leveraging network technology, Internet finance has gained widespread acceptance and offers distinct advantages and characteristics over traditional finance methods. Its inclusive nature, equal participation opportunities, and convenient modes of operation have contributed to its rapid growth (Mugarura, Norman, & Emma, 2021). Furthermore, several Internet financial enterprises are constantly driving reform and innovation, leading to transformative changes in their operational models within the traditional financial system.

Nevertheless, the impact of Internet finance on the stable development of the financial market cannot be overlooked, as it poses certain challenges (Liu, 2022). In the context of China’s judicial practice, Figure 4 illustrates the key characteristics of Internet finance crimes.

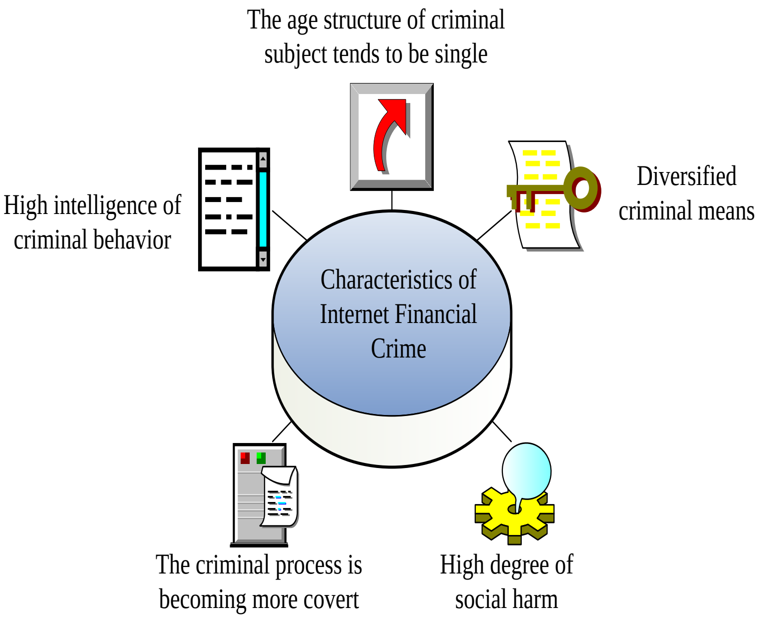

The age structure of criminal subject tends to be single
High intelligence of criminal behavior
Diversified criminal means
Characteristics of Internet Financial Crime
The criminal process is becoming more covert
High degree of social harm

Figure 4. Characteristics of Internet finance crime

Figure 4 demonstrates key characteristics of Internet finance crimes, including the sophisticated nature of criminal behavior, a tendency for single-age structures among perpetrators, diverse methods employed in committing the crimes, a covert criminal process, and significant social harm (Hidajat, 2020). Internet financial crimes not only disrupt the normal functioning of the financial market but also jeopardize public property security (Peurink, 2018). Finance is typically associated with security, profitability, and liquidity, while the Internet is known for its openness, efficiency, and convenience (Mugarura et al., 2021). The combination of these two domains requires a balance between security and openness.

Types of Internet Financial Crimes

A new development trend is emerging in the financial sector, highlighted by the advent of Internet finance as a novel business form. Internet finance, facilitated by network technology, embodies the principles of openness, equality, cooperation, and sharing (Tang et al., 2019). It operates at low costs and has simplified processes. However, despite its numerous advantages, Internet finance also brings various challenges, primarily due to regulatory limitations and legal restrictions (Liu, 2022). Figure 5 illustrates the different types of Internet finance crimes that exist in this context.

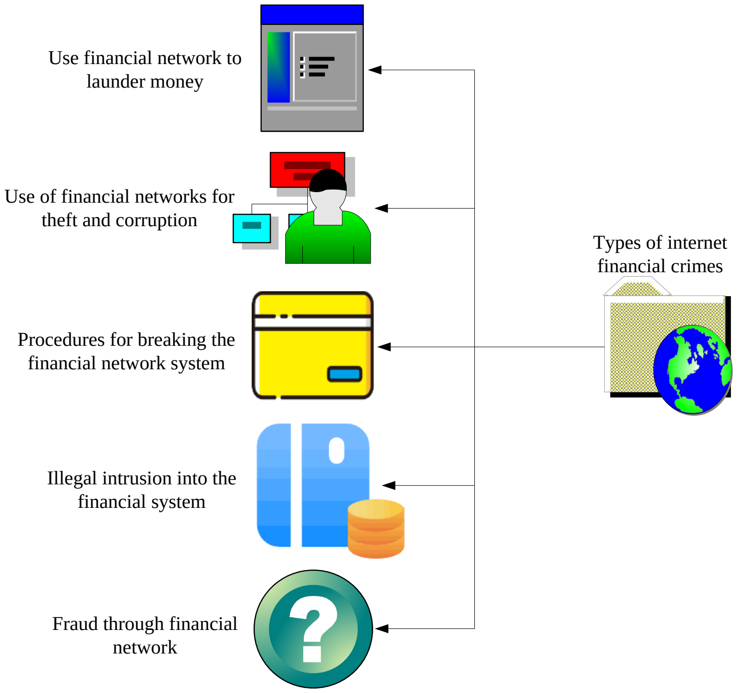

Use financial network to launder money
Use of financial networks for theft and corruption
Procedures for breaking the financial network system
Illegal intrusion into the financial system
Fraud through financial network
Types of internet financial crimes

Figure 5. Types of Internet finance crimes

Figure 5 provides an overview of the various types of Internet finance crimes, including fraudulent activities conducted through financial networks, money laundering via financial networks, theft and corruption facilitated by financial networks, illegal intrusion into financial systems, and tactics for breaching financial network security (Xu, Zhang, & Chen, 2018). Among these, financial network fraud stands out as the most prevalent form of financial crime. Specifically, credit card fraud is a common occurrence, involving the illicit use of electronic currency that is issued to customers following bank credit assessment, and is intended for consumption purposes (Haqq & Gideon, 2019). In today's digital era, credit cards have become an essential payment method in people’s lives, and unfortunately, their misuse for fraudulent activities has become a regular occurrence (Deliema, 2020).

Big Data Based on Data Processing

In today’s era, the growth and advancement of Internet finance, including online shopping platforms, Internet banking, and various forms of Internet-based credit cards, have expanded rapidly. Concurrently, criminal activities like Internet theft and fraud have also increased (Akdemir et al., 2020). Criminals employ unlawful methods to infiltrate financial network information systems and manipulate relevant account information for illicit purposes. As the amount of Internet finance data continues to increase, data processing becomes crucial for analysis and understanding (Kshetri, 2019). Figure 6 illustrates the operational framework for data processing in this context.

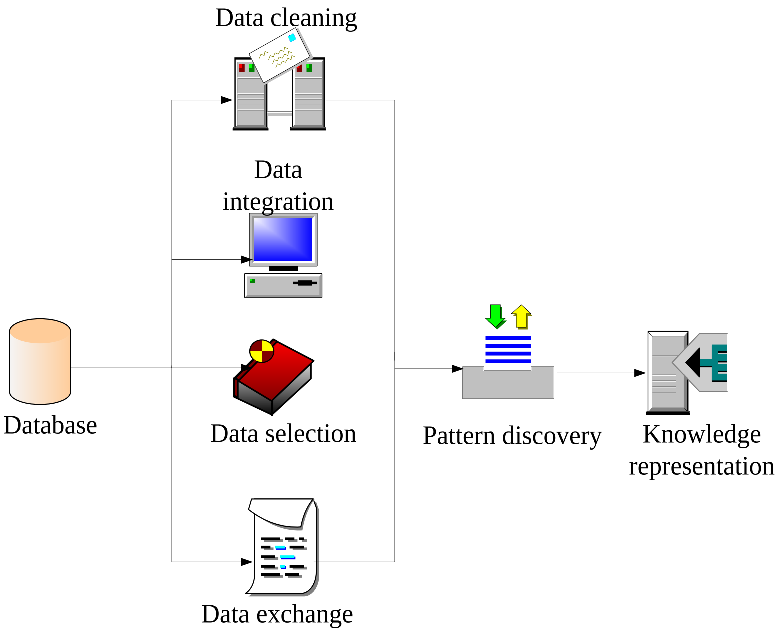


Figure 6. Working principle of data processing

Figure 6 demonstrates the functioning principle of data processing, which involves various stages such as data cleaning, data integration, data selection, and data exchange. Subsequently, pattern discovery is conducted to represent knowledge based on the processed data. The realm of Internet finance is plagued by a substantial number of fraud cases, with specialized intermediaries even emerging to facilitate such fraudulent activities. These intermediaries possess in-depth knowledge of Internet lending platforms' auditing procedures. As a preventative measure against Internet financial crimes, utilizing big data to extract relevant information from Internet behavior data is crucial. Predicting criminal acts and conducting correlation analyses of such activities are significant in managing Internet finance crimes (Nindito, 2018).

Crime Prediction based on Random Forest

Random Forest is an innovative fusion algorithm that combines the concepts of Decision trees and Bagging. Its primary objective is to enhance the performance of Decision trees. During the training phase, each tree extracts relevant data independently, and their distributions remain consistent. However, due to the diverse classification abilities of the individual trees and their inherent correlation, classification errors can occur. Nevertheless, by generating multiple Decision trees randomly, these issues can be effectively resolved. The resulting classifier derived from the random forest algorithm exhibits excellent predictive capabilities, particularly when faced with challenges such as missing data and imbalanced datasets (What is Random Forest, n.d.).

The random forest algorithm possesses several advantages. It exhibits strong anti-noise capability, achieves high recognition accuracy, and serves as a basis for variable sorting and screening. Additionally, it offers valuable insights into interpreting practical problems (Hu & Szymczak, 2023).

1) Decision tree algorithm

The Decision tree serves as the fundamental building block of the random forest algorithm and leverages probability and statistical methods. It functions as a predictive model applicable in various domains, including the prediction of crime categories and severity levels in Internet finance. By utilizing a Decision tree, a clear association between specific attributes of Internet finance and their corresponding values can be demonstrated. Starting at the root node, which is divided based on different user attributes, the Decision tree progresses through various nodes until reaching the leaf node. This ultimately determines the final classification outcome (What is Random Forest, n.d.).

The concept of information gain is derived from the alteration in information entropy. Prior to selecting user attributes, it is necessary to estimate the information. Let's consider a sample ***D***, wherein there exist crimes belonging to category ***c***. The information entropy formula, which is utilized before the growth of a node, can be expressed as follows (Huang, 2021):

$$Info(D) = -\sum_{i=1}^{c} p_i \log_2(p_i) \text{(1)}$$

When a user attribute is chosen as the condition for node growth in sample ***D***, the information entropy of the dataset within that attribute can be expressed as: ***InfoA(D)***, and its calculation formula is as follows (Huang, 2021):

$$Info_A(D) = -\sum_{j=1}^{k} \frac{|D_j|}{D} * Info(D_j) \text{(2)}$$

When influenced by attributes, the information entropy of ***D*** decreases, and its calculation formula is as follows (Huang, 2021):

$$Gain(A) = Info(D) - Info_A(D) \text{(3)}$$

In the growth process of a decision tree, the attribute that is most suitable to be the judgment condition on a node is the attribute with the highest ***Gain(A)*** value (Huang, 2021).

2) Bagging integration algorithm

The Decision tree demonstrates effectiveness in classifying criminal behaviors. However, individual trees are relatively inaccurate, and issues such as over-fitting are present. To address these challenges, the Bagging algorithm, also known as Bootstrap Aggregating, was introduced as a solution (Tsymbal & Puuronen, 2000). The Bagging algorithm was specifically designed to overcome these limitations. The Gini coefficient serves as a method to quantify the level of data impurity. In the context of financial behavior, $\boldsymbol{p_i}$ is used to denote the percentage of financial crimes within the entire dataset (Song et al., 2020).

$$Gain(D) = 1 - \sum_{i=1}^{c} p_i^2 \text{ (4)}$$

Based on this equation, a higher Gini coefficient indicates lower information purity. In the case of sample ***D***, when a specific user attribute is used as the condition for node expansion, the Gini coefficient of the dataset pertaining to that attribute can be determined (Song et al., 2020).

$$Gain_A(D) = -\sum_{j=1}^{k} \frac{|D_j|}{D} * (D_j) \text{(5)}$$

The updated dataset may contain duplicate values from the original dataset. Likewise, to maintain consistency with the sample values, certain values from the original dataset may not be present in the revised dataset.

Association Rule Analysis

As Internet finance continues to advance, the amount of available data also grows substantially. To effectively handle such vast amounts of data, association rule analysis becomes essential. By employing association rules, it becomes possible to analyze, predict, and prevent criminal activities. This analysis involves uncovering intrinsic connections from past cases, determining their overarching characteristics, and subsequently conducting analysis and predictions. Ultimately, this approach can offer new leads and support for future investigative efforts (Anisha, 2018). Association rules play a significant role in data mining. In recent times, there has been a continuous influx of efficient algorithms aimed at extracting association rules. Nevertheless, given the challenge of handling large volumes of data, there is a need to enhance intelligent processing and analysis technologies for data. Further advancements in this area are crucial to addressing this concern (Anisha, 2018).

Consider ***T*** as the collection of all transactions, where each transaction ***t_i*** contains an item set that is a subset of ***i***. The width of a transaction refers to the count of items within that transaction. The support ***σ(A)*** of an item set ***A*** can be mathematically represented as per Yin (2022):

$$\sigma(A)=\left|\{t_i \mid A\subseteq t_i, t_i\in T\}\right| \quad (6)$$

The symbol ***Φ*** represents the number of elements in a set, and the association rule is the logical implication of ***A∩B*** (Yin, 2022):

$$A\cap B=\phi \quad (7)$$

Generally, the strength of the rule depends on the support and confidence. Support refers to the number of times a given data set appears in the whole transaction, while confidence refers to the percentage of A and B data sets included in the whole transaction. Support ***S(A→B)*** and confidence ***C(A→B)*** are defined as follows (Yin, 2022):

$$S(A\rightarrow B)=\frac{\phi(A\cup B)}{N} \quad (8)$$

$$c(A\rightarrow B)=\frac{\phi(A\cup B)}{\phi(A)} \quad (9)$$

In practical scenarios, when both the support and confidence values align, it is referred to as a strong association. The primary challenge lies in establishing association rules that not only satisfy the minimum support requirement but also surpass the predefined threshold. The goal is to generate rules that exhibit higher support values than the specified threshold.

Research Methodology

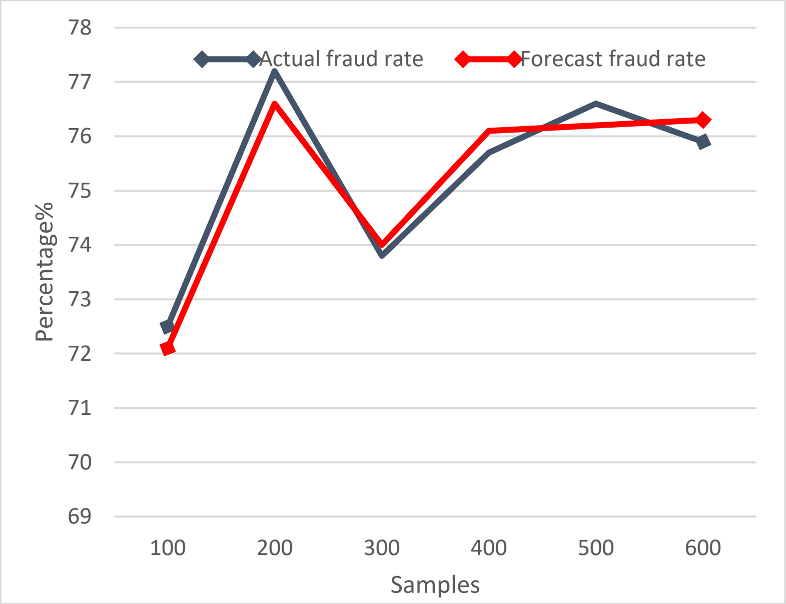
This paper adopts a quantitative research methodology. Quantitative research methodology refers to scientific research to determine the stipulation of certain aspects of things (Nikita, 2020). It is a research method and process that expresses problems and phenomena with quantities, and then analyzes, tests, and explains them to obtain meaning. Quantification is to measure based on digital symbols (Nikita, 2020). Quantitative research measures the characteristic value of the object by comparing the characteristics of the research object according to a certain standard or finding out the change law of the quantity between certain factors (Nikita, 2020). Because its purpose is to answer the quantitative properties of things and their movements, it is called quantitative research. Quantitative research is closely related to scientific experimental research. It can be said that scientific quantification is accompanied by experimental methods (Nikita, 2020). The main methods of quantitative research design are the survey method, correlation method, and experimental method. The experimental method refers to a research method that manipulates one or more variables and controls the research environment to measure the causal relationship between the independent variable and the dependent variable. There are two kinds of experimental methods, one is the natural experiment method, and the other is the laboratory experiment method (Nikita, 2020).

Random forest algorithms include the Decision tree algorithm and the Bagging integration algorithm. Applying the computer algorithm combination of random forest algorithms and association rule analysis to “Research on Legal Supervision of Internet Financial Crime” is the quantitative research. This is because large amounts of data and variables can be analyzed and processed using these algorithms to generate quantitative results and conclusions. Through quantitative analysis of data, it is possible to quantitatively evaluate Internet financial crime. This is done by establishing predictive models and formulating corresponding legal and regulatory measures.

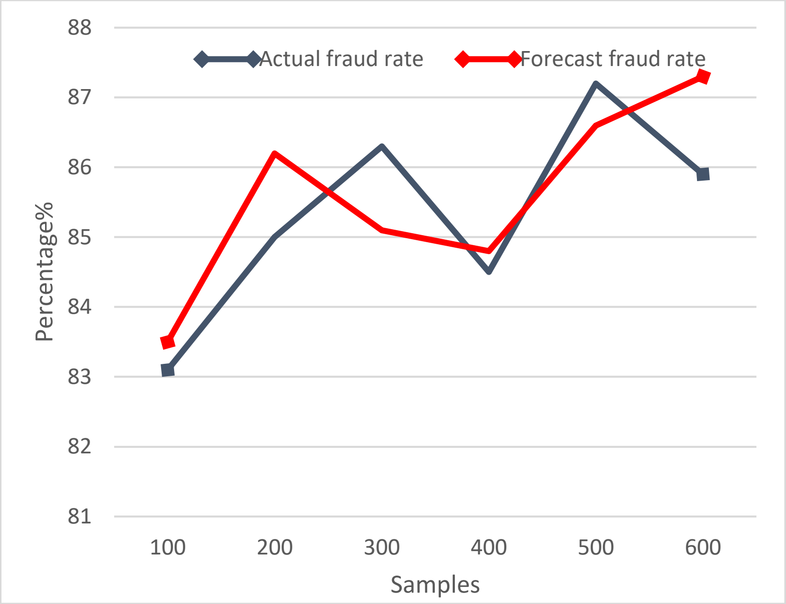
Results and Discussion

Results of Crime Prediction Based on Random Forest

In the experiment, a total of 1200 crime samples were collected, which were then divided into two sets: test samples consisting of 600 data points and experimental samples also comprising 600 data points. These samples were analyzed to assess the predictive capabilities of the model by comparing the actual crime rate with the predicted crime rate in each group. Figure 7 showcases the actual crime rate and the predicted crime rate of the random forest technique across different sample sets:



(a) Actual crime rate and random forest predicted crime rate under test sample



(b) Actual crime rate and random forest predicted crime rate under the experimental sample

Figure 7. Actual crime rate and random forest predicted crime rate under different samples

As depicted in Figure 7, the analysis reveals the following observations

(a) In the case of the test sample, when the sample size is 100, the actual crime rate and predicted crime rate of the random forest model are 72.5% and 72.1%, respectively. For a sample size of 200, the actual crime rate and predicted crime rate are 77.2% and 76.6%, respectively. Similarly, for a sample size of 300, the actual crime rate and predicted crime rate are 73.8% and 74%, respectively. Finally, when the sample size reaches 600, the actual crime rate and predicted crime rate are 75.9% and 76.3%, respectively.

(b) The experimental sample, as shown in Figure 7(b), demonstrates that for a sample size of 100, the actual crime rate and predicted crime rate of the random forest model are 83.1% and 83.5%, respectively. When the sample size increases to 400, the actual crime rate and predicted crime rate become 84.5% and 84.8%, respectively. Further, for a sample size of 600, the actual crime rate and predicted crime rate are 85.9% and 87.3%, respectively. Notably, the random forest model generally exhibits a higher crime rate prediction for both the test samples and the experimental samples.

Results of Crime Prediction Based on Association Rules

In response to various requirements, this paper proposes an analytical approach to exploring the association rules among criminal acts, with a specific emphasis on identifying the interconnectedness of such acts. By extrapolating from the novel patterns and characteristics of criminal behavior, this method aims to infer the likelihood of recidivism among offenders, ultimately contributing to crime prevention and control efforts. The correlation analysis of financial crimes is presented in Table 3, highlighting the findings.

Table 3
Correlation analysis of financial crimes

Number of samples	Test sample	Experimental sample
100	0.89	0.93
200	0.93	0.92
300	0.90	0.96
400	0.91	0.95
500	0.94	0.94
600	0.92	0.97

As illustrated in Table 3, the correlation analysis demonstrates the following results:

For a sample size of 100, the correlation degree between the test samples and experimental samples is 0.89 and 0.93, respectively. With a sample size of 200, the correlation between the test sample and the experimental sample is 0.93 and 0.92, respectively. When the sample size increases to 300, the correlation between the test sample and the experimental sample becomes 0.90 and 0.96, respectively. Furthermore, for a sample size of 400, the correlation between the test sample and the experimental sample is 0.91 and 0.95. Finally, with a sample size of 600, the correlation between the test sample and the experimental sample is observed to be 0.92 and 0.97, respectively.

This exploration of various types of criminal laws enables a deeper understanding of specific groups of criminal acts, enhancing efforts to prevent their occurrence. By combining association rules with the expertise of public security and judicial departments, not only can the utilization of information be improved, but new patterns can also be timely uncovered.

Countermeasures for Legal Regulating of Internet Financial Crime

1) Enhance the legal framework for Internet finance

The continuous advancements and transformations brought about by the Internet have also created opportunities for criminals in the realm of Internet finance. Over the years, the frequency and variety of Internet financial crime have increased, posing a significant threat to China's economy and society. From a legal standpoint, the challenges faced by Internet finance are substantial. During the initial stage of Internet finance development, it is essential to establish a robust legal foundation, clarifying its innovative legal positioning while demonstrating its specific legitimacy. Simultaneously, adopting an open-minded approach to legal thinking and methods becomes crucial.

Relevant authorities should draft and implement regulations focusing on the management content and strategies pertaining to Internet finance, emphasizing the need for further improvements in legislation. By ensuring compatibility, the constituent elements of Internet finance can be defined, and new criteria can be added to the existing legal system. Through comprehensive coordination, in-depth investigations, and thoughtful considerations specific to Internet finance, a comprehensive legal framework can be established, bringing about standardization and guidance.

2) Enact dedicated legislation to address Internet financial crime in China

Presently, China's regulations pertaining to Internet financial crime are minimal and suffer from various deficiencies, hindering effective measures against Internet financial crimes. The emergence of new forms of Internet financial crime has extended beyond the purview of traditional criminal law for financial derivatives crimes. Existing financial laws primarily focus on criminal liability and often do not apply to these newly arising financial crimes, leading to limited convictions.

To tackle the novel challenges introduced by Internet financial crime and incorporate fresh legal concepts, it is imperative for relevant legislative bodies to conduct scientific research on the potential risks associated with the open nature of Internet finance. In cases where Internet financial crime severely endangers society and the financial order, timely and decisive actions must be taken to effectively combat them. Consequently, it becomes necessary to regulate existing types of Internet financial crime and make specialized legislation specifically addressing Internet financial crime in China.

Conclusion

The results indicate that both random forest algorithms and association rules exhibit significant predictive capabilities in both test and experimental samples. Consequently, the application of a computer algorithm combination involving random forest algorithms and association rule analysis proves to be effective in predicting Internet financial crime.

Behind the rapid growth of Internet finance lies a multitude of criminal activities, highlighting the emerging nature of this industry. In recent years, Internet finance has disrupted traditional modes of financial transactions. However, given the imperfections in Internet financial platforms and regulatory frameworks, some Internet financial companies have taken advantage of financial innovation as a cover to engage in fraudulent activities. These activities include financial scams and illegal fundraising. These criminal acts pose significant challenges to the Internet finance industry. Therefore, finding effective solutions to prevent and combat Internet finance crimes and ensure the smooth operation of this sector has become a pressing issue. Addressing this challenge requires not only the enhancement of relevant laws, regulations, and judicial interpretations but also the strengthening of network information prevention technologies. By increasing the costs associated with committing such crimes, individuals, and organizations engaged in Internet finance's criminality can be deterred, leading to greater security and integrity within the industry.

Acknowledgement

The assistance of Dr. Hanna Binti Ambaras Khan and Prof. Dr. Suhaimi Bin Ab. Rahman was instrumental in the completion of this paper. I extend my heartfelt appreciation for their guidance and support throughout the entire research process. Their invaluable input and expertise have played a pivotal role in the accomplishment of this paper.

References

Abdullah, W. N., & Said, R. (2019). Audit and risk committee in financial crime prevention. Journal of Financial Crime, 26(1), 223-234.

Akdemir, N., & Lawless, C. J. (2020). Exploring the human factor in cyber-enabled and cyber-dependent crime victimization: A lifestyle routine activities approach. Internet Research, 30(6), 1665-1687.

Amjad, R. M. (2022). Non-linear impact of globalization on financial crimes: A case of developing economies. Journal of Money Laundering Control, 25(2), 358-375.

Anisha, D. (2018). Association Rules. GeeksforGeeks. Retrieved July 11, 2023, from www.geeksforgeeks.org/association-rule/.

Brands, J., & van Wilsem, J. (2021). Connected and fearful? Exploring fear of Internet financial crime, Internet behavior and their relationship. European Journal of Criminology, 18(2), 213-234.

DeLiema, M. (2020). Financial fraud among older Americans: Evidence and implications. The Journals of Gerontology: Series B, 75(4), 861-868.

Haqq, A. P. N. A., & Budiwitjaksono, G. S. (2019). Fraud pentagon for detecting financial statement fraud. Journal of Economics, Business, and Accountancy Ventura, 22(3), 319-332.

Hidajat, T. (2020). Unethical practices peer-to-peer lending in Indonesia. Journal of Financial Crime, 27(1), 274-282.

Hu, J., & Szymczak, S. (2023). A review on longitudinal data analysis with random forest. Briefings in Bioinformatics, 24(2), bbad002.

Huang, K. (2021). Decision Tree, Medium. Available at: https://medium.com/%E4%BA%BA%E5%B7%A5%E6%99%BA%E6%85%A7-%E5%80%92%E5%BA%95%E6%9C%89%E5%A4%9A%E6%99%BA%E6%85%A7/decision-tree-%E6%B1%BA%E7%AD%96%E6%A8%B9-%E5%96%AE%E7%B4%94-%E5%BF%AB%E9%80%9F-%E8%A7%A3%E9%87%8B%E6%80%A7%E9%AB%98%E7%9A%84%E6%B1%BA%E7%AD%96%E8%A1%93-ef28e0e75a55 (Accessed: July 11, 2023).

Kshetri, N. (2019). Cybercrime and cybersecurity in Africa. Journal of Global Information Technology Management, 22(2), 77-81.

Liu, X. (2022). Internet Financial Crime Research. Shanghai Ren Min press.

Mugarura, N., & Ssali, E. (2021). Intricacies of anti-money laundering and cyber-crimes regulation in a fluid global system. Journal of Money Laundering Control, 24(1), 10-28.

Nikita, T. (2020). Quantitative Research vs. Qualitative Research: How to Choose? Editage Insights. Retrieved from www.editage.cn/insights/ding-liang-yan-jiu-yu-ding-xing-yan-jiu-ru-he-xuan-ze-5524.

Nindito, M. (2018). Financial statement fraud: Perspective of the Pentagon Fraud model in Indonesia. Academy of Accounting and Financial Studies Journal, 22(3), 1-9.

Reurink, A. (2018). Financial fraud: a literature review. Journal of Economic Surveys, 32(5), 1292-1325.

Song, Y., et al. (2020). An Improved C4.5 Algorithm in Bagging Integration Model. IEEE Access, 8, 206866-206875.

Tang, J., & Karim, K. E. (2019). Financial fraud detection and big data analytics–implications on auditors’ use of fraud brainstorming session. Managerial Auditing Journal, 34(3), 324-337.

Teichmann, F. M. J., & Falker, M. C. (2021). Cryptocurrencies and financial crime: solutions from Liechtenstein. Journal of Money Laundering Control, 24(4), 775-788.

Tsymbal, A., & Puuronen, S. (2000). Bagging and boosting with dynamic integration of classifiers. In Principles of Data Mining and Knowledge Discovery: 4th European Conference, PKDD 2000 Lyon, France, September 13–16, 2000 Proceedings 4 (pp. 116-125). Springer Berlin Heidelberg.

Wronka, C. (2022). Impact of COVID-19 on financial institutions: Navigating the global emerging patterns of financial crime. Journal of Financial Crime, 29(2), 476-490.

Xu, Y., Zhang, L., & Chen, H. (2018). Board age and corporate financial fraud: An interactionist view. Long Range Planning, 51(6), 815-830.

Yang, D. (2018). Internet finance: Its uncertain legal foundations and the role of big data in its development. Emerging Markets Finance and Trade, 54(4), 721-732.

Yin, C. (2022). Association Rules Mining, Frequent Set Mining, and Aporiori. Blog.csdn.net. Retrieved from blog.csdn.net/qq_43391414/article/details/109326990.