Research on the Identification and Early Warning Model of College Students' Cybercrime Behavior Characteristics Based on Data Mining

Jinbo Li
Department of History, Culture and Law, Tangshan Normal University, Tangshan 063009, Hebei, China
Corresponding author: Jinbo Li (e-mail: 17746275859@163.com)

ABSTRACT To overcome the limitation that traditional models fail to capture deep correlations in college students' online behaviors, this paper proposes an early-warning model for cybercrime behavior characteristics based on multi-source data mining and deep graph learning. First, internet browsing logs, campus-card consumption records, dormitory access-control data, and psychological assessment data are integrated to construct a behavioral feature database. Second, a dynamic community graph is built using spatial co-occurrence, consumption similarity, and course-overlap relationships. Third, a heterogeneous graph attention network is used to extract behavioral transmission characteristics in student social networks. Finally, a risk-identification module is constructed for early warning. Experiments on anonymized campus data show that the model achieves 91.3% accuracy and 90.5% recall, with an early-warning lead time of 6.5 days compared with LSTM-based methods. The results verify the effectiveness of the proposed model in deep feature mining, risk recognition, and proactive cybercrime prevention in campus network governance.

INDEX TERMS cybercrime behavior, data mining, heterogeneous graph neural network, early warning, campus network security

I. INTRODUCTION

WITH the deep penetration and widespread application of Internet technology in higher education, the online behavior of college students has become increasingly complex. In recent years, cases of college student cybercrime involving campus loan fraud, online gambling, hacking, and personal information trafficking have occurred frequently, showing new characteristics of intelligent methods, concealed behavior, and organized crime [1,2]. However, the network security protection system of most universities is still based on fixed rule firewall interception and post-event log auditing, which has two major pain points: First, the analysis of network behavior data is limited to shallow indicators such as single-point login frequency and traffic statistics, lacking the mining of deep correlation characteristics such as students' social relationships, time series patterns, and changes in psychological state; second, the existing early warning models are mostly static threshold triggering mechanisms, which are difficult to capture the diffusion path and evolution trend of criminal behavior in social networks in a timely manner, resulting in delayed early warning and high false alarm and false alarm rates [3]. Therefore, constructing a college student cybercrime early warning model that can deeply integrate multi-source data and accurately identify deep behavioral characteristics has become a key issue in improving the governance capacity of campus cyberspace.

At present, scholars at home and abroad have carried out a lot of research on college student network behavior analysis and risk early warning. Based on students' basic information, grades and online learning data, Li and Zhou constructed an academic early warning system combining GBCFSFDP clustering and WNBC-FOA classification algorithm to identify abnormal learning behaviors and improve the effectiveness of academic management [4]. Al-Badayneh et al. used 500 students from four universities in Jordan as a sample to examine the attribution differences in college students' knowledge of Jordan's cybercrime law [5]. Mwiraria et al. used students from Egerton University in Kenya as a sample to explore the impact of personal attributes such as gender, age and academic level on college students' risk of suffering from different types of cybercrime [6]. Balogun et al. used undergraduates from the University of Elorin to study the prevalence of cybercrime, participation factors and its impact, and proposed to curb college students' cybercrime through education, awareness enhancement and policy

implementation [7]. Based on survey data of 1,037 college students in China, Lin et al. found that daily online activities mainly predict attempted victims of telecommunications network fraud, while victims who actually suffer economic losses are more affected by factors such as target suitability and low self-control [8].

However, a comprehensive analysis of existing research reveals that most studies focus only on the superficial statistical characteristics of individual behavior, failing to fully explore the impact of social connections among students on the transmission of criminal behavior. Then, this paper proposes a new kind of early warning method based on multi-source behavioral features and deep graph learning to solve the problem of shallow deep-level feature mining in traditional models. Firstly, a three-dimensional feature system of "individual-community-time series" is constructed. The multisource data, including students' online log, consumption record and psychological assessment, are transferred into computable graph structure. Secondly, an improved graph convolutional network is used to construct a dynamic behavioral association graph based on the relationships of same-dormitory, same-course and same-consumption, and further describe the transmission and evolution pattern of criminal feature in social network. Then, a heterogeneous graph fusion module based on attention mechanism is designed to automatically and weightedly fuse explicit behavioral feature and implicit psychological state feature. Finally, a temporal attention network is constructed to globally model behavioral trajectory and realize early and accurate recognition of high-risk behavior. Through the technical route, this study aims to realize "from post-event tracing to pre-event prevention", and enhance the intelligence level of campus cybercrime early warning.

II. PREPROCESSING AND FEATURE LIBRARY CONSTRUCTION OF MULTI-SOURCE CAMPUS BEHAVIORAL DATA

The data in this study was collected from an anonymized data set released by the IT office of a university from September 2021 to January 2024, including the daily behavior data of 21,000 undergraduate and graduate students from all colleges of the university. The data types are mainly four kinds as follows:

1) Internet authentication log: the time of starting and ending internet connection, IP address and URL of the site visited by students;

2) Campus card consumption record: the time, money and location of buying canteen, supermarket and bathroom;

3) Dormitory access control data: the time and the building number of students entering and leaving the dormitory building; and

4) Psychological assessment scale: collected once a semester, including the score of anxiety, depression, interpersonal sensitivity, etc.

All the data are identified by student ID number. However, to protect students' privacy, anonymization was implemented on the original data set released by the university. Student ID number was replaced by random code. In addition, the name and ID card number were removed. Data preprocessing mainly includes three steps. First, data cleaning was performed: For duplicate records in internet browsing logs caused by network interruptions, a timestamp deduplication algorithm was used to retain the first occurrence of the data; refund entries with negative amounts in the campus card transaction records were removed; for redundant records in access control data showing multiple entries and exits to the same building within the same minute, only the first entry/exit time was retained. Regarding missing value handling, for individual unanswered questions in the psychological assessment scale, the average of the student's major and class was used to fill in the missing values; for students with no internet browsing logs for three consecutive days, their internet usage time was set to zero and they were marked as low-activity samples.

Second, time alignment and slicing were performed: Due to the different timestamp precision of various data sources (internet browsing logs are accurate to the second, access control data to the minute), timestamps were standardized to the "year-month-day-hour" format, and continuous behavior was segmented into behavioral segments on a daily basis for easier feature extraction. Finally, outlier detection was performed: the Isolation Forest algorithm was used to identify outliers in each data dimension, such as extreme values like daily internet usage exceeding 20 hours. While single transaction amounts exceeding 5 times the standard deviation were flagged, these were not automatically removed, as they often represent legitimate large-scale student expenditures (e.g., tuition or electronics) or critical financial anomalies indicative of cybercrime involvement. Samples confirmed by manual review to be due to equipment malfunction or account theft were removed.

The construction of the feature library revolves around a multi-dimensional characterization of individual behavior. Features extracted from internet browsing logs include: average daily internet usage time, percentage of internet usage time during late night hours, distribution of accessed domain categories (education, entertainment, social networking, gambling, etc.), and keyword hit frequency based on URL content. The keyword library, provided by the campus network security department, covers sensitive words related to cybercrime such as "circumventing the Great Firewall," "hacker," "bombing," and "click farming," and uses natural language processing technology to segment and match URL titles and page summaries. Consumption pattern features are extracted from campus card spending records: daily spending frequency, monthly spending fluctuation coefficient, the consistency of daily consumption time-intervals (reflecting temporal regularity while accounting for varied individual habits such as skipping meals), and consumption location entropy (measuring the diversity of consumption locations). Regularity pattern features are extracted from dormitory access control data: first departure time of the day, latest

return time, and frequency of nighttime outings. Raw scores and norm reference scores for four dimensions–anxiety, depression, hostility, and paranoia–are directly extracted from psychological assessment scales. After standardization, these features form a 187-dimensional individual behavior feature vector. The feature vectors of all students together constitute the feature library, serving as the basic input for subsequent graph structure modeling.

III. CONSTRUCTION OF A DYNAMIC CAMPUS COMMUNITY GRAPH BASED ON SPATIOTEMPORAL RELATIONSHIPS

To explore the transmission characteristics and gang-related patterns of cybercrime among university students at the group level, this study analyzes individual students within a dynamic network of social relationships. The construction of the dynamic community graph in this study is based on two core dimensions: physical spatial co-occurrence relationships and behavioral pattern similarity. Physical spatial co-occurrence relationships are primarily characterized by Wi-Fi access point locations and dormitory access control records. Specifically, the location information of each student's internet access point is extracted from the campus network authentication logs. When two students access the same Wi-Fi base station at the same time, it is considered a spatial co-occurrence. Dormitory access control data records the times students enter and exit dormitory buildings. If two students live in the same building and their first departure time or latest return time each day highly overlaps, they are also considered to have a physical spatial relationship.

Behavioral pattern similarity is extracted from consumption records and course selection information. Regarding consumption records, the frequency of two students appearing at the same cafeteria window during the same time period (such as lunchtime on the same day) is calculated; the higher the frequency, the stronger the behavioral similarity. Regarding course selection information, the number of courses jointly selected by two students is used as one of the indicators to measure the overlap of their activity trajectories. After completing the above-mentioned correlation dimension calculations, this study uses the Jaccard similarity coefficient to fuse multi-dimensional correlations. Taking student i and student j as examples, the formula for calculating their comprehensive behavioral correlation weight W_{ij} is defined as (1):

$$W_{ij} = \alpha \cdot J_{spatial}(i,j) + \beta \cdot J_{consumption}(i,j) + \gamma \cdot J_{course}(i,j) \quad (1)$$

Where $J_{spatial}(i,j)$ represents the ratio of the number of times the two students co-occur in space within the time window to the total number of times they appear independently, $J_{consumption}(i,j)$ represents the similarity coefficient of consumption co-occurrence, and $J_{course}(i,j)$ represents the similarity coefficient of course selection overlap. α, β, γ are weight coefficients, determined through grid search optimization. In this study, the final values are $\alpha = 0.4$, $\beta = 0.3$, $\gamma = 0.3$. For any two students, if the combined weight W_{ij} exceeds a preset threshold (determined to be 0.3 after multiple trials), an edge is established between them, with the edge weight being W_{ij}.

It is worth mentioning that campus community relationships are dynamic. Students' activity trajectories and behaviors may vary with different semesters, different courses and even different friends. To capture such dynamics, this study uses a sliding time window method to build a dynamic community graph. We define the time window as 30 days and slide 15 days every time. For each time window, the behavioral association weights between students are calculated independently. To address the 'vacation gap' or 'cold start' problem during winter and summer breaks–when campus logs naturally cease–the sliding window mechanism is suspended during non-session periods and re-initialized upon the start of the new semester to ensure data continuity is not artificially fragmented. That is, the graph structure of the same student group may be different in different time windows. For example, at the beginning of the semester, people with overlapping course selections may be more likely to form a community; during the semester, people who co-occur more times while consuming may be more likely to form a community; around the exam week, people who co-occur more times while going to the library may be more likely to form a community. By this way, the model could model the evolution of behavioral relationships over time and be more close to real campus life.

IV. DEEP FEATURE REPRESENTATION BASED ON HETEROGENEOUS GRAPH ATTENTION NETWORK (HAN)

After completing the construction of individual behavior feature base library and dynamic community graph modeling, mining deep semantic features based on effectively integrating multi-dimensional information plays an important role in improving the performance of early warning model. Traditional graph convolutional networks achieve optimal performance on homogeneous graphs. However, in the community graph constructed in this paper, the edges between nodes are not of the same type, but cover various kinds of relationships, such as space co-occurrence relationship, consumption similarity relationship and course overlap relationship. These different types of relationships contain different semantic information. For example, space co-occurrence may represent the intersection of daily life circle, consumption similarity may represent the convergence of economic behavior and course overlap may represent the similarity of learning route.

In order to capture the impact of different types of relationships on criminal behavior identification automatically, this paper constructs a heterogeneous graph attention network, which learns the importance weight of different relationships and different neighboring nodes based on hierarchical attention mechanism automatically. The heterogeneous graph is defined as $G = (V, E, R)$, where V

represents the set of student nodes, E represents the set of edges, and R represents the set of relationship types. In this study, the relation types include three categories: "spatial co-occurrence," "consumption similarity," and "course selection overlap," with each relation corresponding to a meta-path. A meta-path is a composite relation sequence connecting two nodes; for example, "student-spatial co-occurrence-student" represents a pair of students connected through a spatial co-occurrence relation. For each meta-path Φ, the set of neighboring nodes N_i^{Φ} under that relation can be extracted.

The first layer of the model is node-level attention, which aims to learn the influence weight of neighboring nodes on the central node under a specific meta-path. For the central node i, its node-level attention weight under meta-path Φ is calculated as follows (2):

$$\alpha_{ij}^{\Phi} = \frac{\exp\left(\text{LeakyReLU}\left(\mathbf{a}_{\Phi}^{\top}[\mathbf{h}_i \| \mathbf{h}_j]\right)\right)}{\sum_{k \in N_i^{\Phi}} \exp\left(\text{LeakyReLU}\left(\mathbf{a}_{\Phi}^{\top}[\mathbf{h}_i \| \mathbf{h}_k]\right)\right)} \tag{2}$$

Where, $\mathbf{h}_i$ and $\mathbf{h}_j$ are the initial feature vectors of node i and node j (from the feature base library), $\mathbf{a}_{\Phi}$ is the learnable attention parameter corresponding to meta-path Φ, and $\|$ represents the vector concatenation operation. Through this formula, the model can assign a normalized attention coefficient to each neighbor, reflecting its importance to the central node. Subsequently, the neighbor features are weighted and aggregated according to the attention weights to obtain the semantically specific representation of node i under the meta-path Φ, as shown in formula (3):

$$\mathbf{z}_i^{\Phi} = \sigma\left(\sum_{j \in N_i^{\Phi}} \alpha_{ij}^{\Phi} \cdot \mathbf{W}_{\Phi}\mathbf{h}_j\right) \tag{3}$$

$\mathbf{W}_{\Phi}$ is the linear transformation matrix corresponding to the meta-path Φ, and σ is the activation function (ELU is used in this paper). After node-level attention, each node obtains a feature vector that aggregates neighbor information under each meta-path.

The second layer of the model is semantic-level attention, which aims to learn the importance of different meta-paths to the final node representation. Since different types of relationships have different indicative effects on criminal behavior–for example, some crime patterns may rely more on the convergence of consumption behavior, while others may rely more on spatial co-occurrence–it is necessary to automatically assign weights to each meta-path. The semantic-level attention is calculated as follows (4):

$$\beta_{\Phi} = \frac{\exp\left(\frac{1}{|V|}\sum_{i \in V} \mathbf{q}^{\top} \tanh(\mathbf{M}\mathbf{z}_i^{\Phi} + \mathbf{b})\right)}{\sum_{\Phi' \in R} \exp\left(\frac{1}{|V|}\sum_{i \in V} \mathbf{q}^{\top} \tanh(\mathbf{M}\mathbf{z}_i^{\Phi'} + \mathbf{b})\right)} \tag{4}$$

Where $\mathbf{M}$ and $\mathbf{b}$ are learnable parameters, and $\mathbf{q}$ is the semantic-level attention vector. This formula first performs a nonlinear transformation on the representation of all nodes under each meta-path and calculates the average to obtain the global semantic embedding of the meta-path. Then, the weight β_{Φ} of each meta-path is calculated through the attention mechanism. Finally, the fusion representation of node i is the weighted sum of the semantic-specific representations under all meta-paths, as shown in formula (5):

$$\mathbf{z}_i = \sum_{\Phi \in R} \beta_{\Phi} \cdot \mathbf{z}_i^{\Phi} \tag{5}$$

Thus, each student node obtains a high-dimensional feature vector $\mathbf{z}_i$ that integrates multi-dimensional relational information. This vector not only contains the individual's own behavioral characteristics, but also aggregates the influence from different types of neighbors, which can effectively characterize the transmission pattern and gang characteristics of criminal behavior in the community. Finally, $\mathbf{z}_i$ is input into a fully connected layer, and the probability value of the student belonging to the criminal behavior category is obtained through the softmax function. While this study treats cybercrime as a binary classification for initial early warning, it is acknowledged that different criminal behaviors (e.g., hacking vs. fraud) exhibit distinct behavioral signatures; future iterations of the model will aim to incorporate multi-class labeling to distinguish between these specific crime types. The entire heterogeneous graph attention network is trained end-to-end, using cross-entropy loss as the loss function, and L2 regularization is added to prevent overfitting. Through this hierarchical attention mechanism, the model can automatically discover the most valuable relationship types and neighbor nodes for the recognition task, improving the discriminative power and interpretability of the feature representation.

V. MODEL RECOGNITION PERFORMANCE AND EARLY WARNING EFFECTIVENESS EVALUATION

A. EXPERIMENTAL SETUP

To comprehensively verify the effectiveness and practicality of the proposed model, this paper designed three progressive experiments. The experimental configurations are shown in Table 1:

B. OVERALL MODEL RECOGNITION PERFORMANCE COMPARISON EXPERIMENT

To analyze the overall model recognition performance of the proposed heterogeneous graph attention network model in distinguishing cybercrime behavior from university students' behavior, an overall model recognition performance comparison experiment was designed. Logistic regression, support vector machine, random forest, and graph convolutional network were chosen as the baseline model. The five-fold cross validation was implemented with multi-source behavioral data from 21,000 students in a university. Accuracy, recall, and F1-score were selected as the evaluation index to comprehensively compared the overall recognition performance of different models in criminal behavior.

As shown in Figure 1, the proposed early warning model based on heterogeneous graph attention network performed

TABLE 1. Experimental Setup

Category	Configuration	Description
Dataset	21,000 students, 470 million records, 247 positive samples	Time span: 2021.09-2024.01, positive-negative sample ratio 1:5
Feature Dimension	187-dimensional behavioral features	Covering four types of data: internet access, consumption, dormitory access, psychology
Graph Structure	Three relationship types: spatial co-occurrence, consumption similarity, course overlap	30-day sliding window, threshold 0.3
Model Parameters	2-layer GCN, 64-dimensional hidden layer, 4 attention heads	Dropout=0.3, activation function ELU
Training Settings	Adam optimizer, learning rate 0.001, 200 epochs	Early stopping patience=20, five-fold cross-validation
Baseline Models	LR, SVM, RF, GCN, LSTM	Comparative experiments under same data partition
Experimental Environment	Python 3.8, PyTorch 1.12, DGL 0.9.1	NVIDIA Tesla V100 GPU

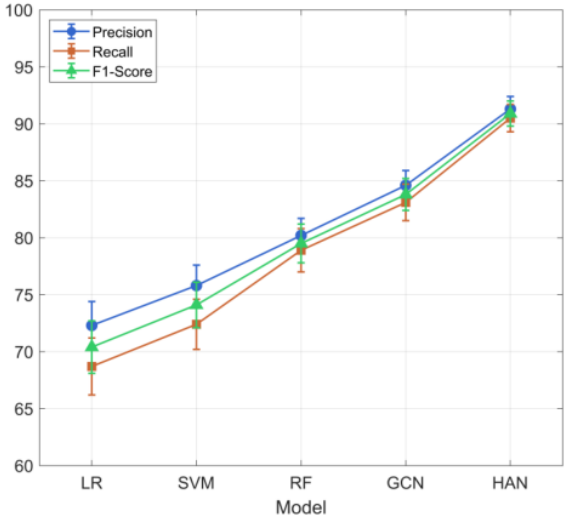

FIGURE 1. Overall Model Recognition Performance Comparison

best across all metrics. The model achieved an accuracy of 91.3%, a recall of 90.5%, and an F1-score of 90.9%, representing improvements of 6.7, 7.4, and 7.1 percentage points respectively compared to traditional graph convolutional networks (GCN). Compared to shallow models such as logistic regression and support vector machine, the performance improvement is more significant, fully validating the effectiveness of integrating multi-source behavioral features and dynamic community graph structures in capturing complex cybercrime behavior patterns. The results demonstrate that our proposed method effectively addresses the shortcomings of traditional models in mining deep relational features, providing reliable support for building accurate early warning systems.

C. ABLATION EXPERIMENT ON THE EFFECTIVENESS OF GRAPH STRUCTURE FEATURES

To further evaluate the effectiveness of dynamic community graph structure in recognition task, we design a graph structure feature ablation experiment. We evaluate three models, i.e., HAN w/o Graph (use only individual behavioral feature and not using any graph structure information), HAN w/ Static (use static administrative class graph), and Full Model (use dynamic behavioral graph in our paper). The three models accuracy, recall and F1-score are compared on the same data set to evaluate the influence of different graph structure information on the performance of crime behavior recognition.

Table 2 shows that graph structure features have a significant impact on model recognition performance. The HAN w/o Graph model using only individual behavior features has an F1-score of 81.5%, while the introduction of a static class graph improves it to 86.3%, indicating that group relationship information can effectively enhance feature representation capabilities. The Full Model using the dynamic behavioral graph constructed in this paper performed best, achieving an F1-score of 90.9%, an improvement of 9.4 percentage points compared to the version without a graph structure and 4.6 percentage points compared to the static graph version. This fully demonstrates that the dynamic community graph constructed based on spatiotemporal co-occurrence and behavioral similarity can more accurately depict the real connections between students, thereby effectively uncovering deep behavioral patterns such as gang-related crimes and reducing the risk of underreporting.

TABLE 2. Ablation Comparison of Graph Structure Feature Effectiveness

Model Variant	Precision (%)	Recall (%)	F1-Score (%)
HAN w/o Graph	82.4 ± 1.6	80.7 ± 1.9	81.5 ± 1.7
HAN w/ Static Graph	86.9 ± 1.3	85.8 ± 1.5	86.3 ± 1.4
Full Model (Dynamic)	91.3 ± 1.1	90.5 ± 1.2	90.9 ± 1.1

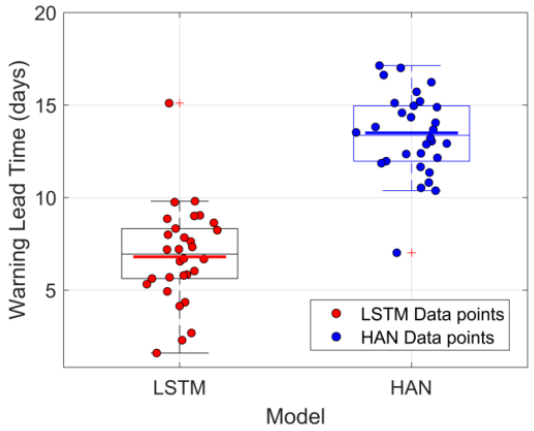

FIGURE 2. Comparison of Early Warning Timeliness and Lead Time

D. COMPARISON EXPERIMENT OF EARLY WARNING TIMELINESS AND LEAD TIME

In order to verify the early warning ability of the model in actual application, an early warning timeliness comparison experiment is designed. Select 30 confirmed cases of college students cybercrime, use the HAN model and LSTM model proposed in this paper to retrospectively predict the behavioral data of 90 days before each case, and record the time when the first high-risk probability output value exceeds the threshold continuously for 3 times. Subtract this time from the time of occurrence of risky behavior. Compare the mean and standard deviation of the two lead times to analyze the difference of early warning ability. It should be noted that while the HAN model benefits from the inclusion of relational graph data which the sequential LSTM does not inherently process, this comparison serves to demonstrate the significant value added by integrating social-relational features into the early warning framework rather than just temporal sequences.

As shown in Figure 2, the HAN model proposed in this paper achieved an average early warning lead time of 13.38 days in 30 risk cases, significantly higher than the 6.88 days of the LSTM model, representing an average improvement of 6.50 days. In terms of stability, the standard deviation of the HAN model's lead time was 2.24 days, lower than the 2.63 days of the LSTM model, indicating a more concentrated distribution of warning time. Paired t-tests showed a statistically significant difference ($p < 0.001$), confirming that the HAN model can capture the evolutionary trend of risky behavior earlier and more stably, gaining valuable intervention time for campus network security management and demonstrating higher practical value.

VI. CONCLUSION

The paper will focus on the issues of inadequate deep feature mining, and the inability to trace gang related crime in the detection of college student cyber-crime behavior. It suggests a multi-source behavioral data based on early warning model which combines deep graph learning and multi-source behavioral information. The model is effective in enhancing the capacity of uncovering obscure and contagious criminal attributes by constructing a dynamic community graph to show the actual behavioral associationism among the students and integrating attention mechanisms to extract patterns of temporal evolution. The experimental findings indicate that the approach is superior in recognition performance and early warning timeliness over the traditional models proving the benefits of multi-source data fusion and graph structure mining in practice. However, even with these positive outcomes, there are still certain weaknesses: the first is that the data sources are largely limited to the specific environment of a single campus,the second is that the dynamic evolution of behavioral features has yet to be fully integrated into a real-time adaptive update system. The future studies will strive to add cross-platform information to increase the variety of samples and research the online learning process so that the model could dynamically change depending on the real-time alterations in the behavioral pattern and improve the intelligence and adaptability of the early warning system.

AUTHOR CONTRIBUTIONS

Jinbo Li designed, collected and analyzed the data, and drafted the manuscript. Jinbo Li conducted the study, critically revised the manuscript for important intellectual content, and gave final approval of the version to be published. Jinbo Li participated fully in the work, take public responsibility for appropriate portions of the content, and agreed to be accountable for all aspects of the work in ensuring that questions related to the accuracy or integrity of any part of the work are appropriately investigated and resolved.

CONFLICTS OF INTEREST

The author declares no conflict of interest.

FUNDING

This research received no external funding.

ACKNOWLEDGEMENTS

Not applicable.

REFERENCES

[1] Y. Xiao and W. Pan, Empirical Study on Countermeasures for College Students to Prevent Telecom Network Fraud: Taking Three Universities in Shenzhen as Examples. Journal of Shenzhen Vocational and Technical College. vol. 21, no. 5, pp. 22-27, 2022. doi: 10.13899/j.cnki.szptxb.2022.05.004

[2] B. Wu, C. Zhou, and S. Ye, The Current Situation, Problems, and Countermeasures of Telecom Network Fraud in Zhejiang Universities: Taking More than 210 Telecom Fraud Cases in A University as an Example. Dispute Resolution. vol. 10, no. 7, pp. 150-161, 2024. doi: 10.12677/ds.2024.107342

[3] S. Zhou, K. Jiang, B. Xu, et al., Research on the Effectiveness Evaluation of Network Security Course Construction for Telecom Network Fraud Governance. Telecommunications Science. vol. 39, no. 6, pp. 122-128, 2023. doi: 10.11959/j.issn.1000-0801.2023127

[4] X. Li and T. Zhou, Design of an online learning early warning system based on learning behaviour analysis. International Journal of Continuing Engineering Education and Life Long Learning. vol. 31, no. 3, pp. 381-393, 2021. doi: 10.1504/IJCEELL.2021.116035

[5] D. M. Al-Badayneh, H. M. A. Dosari, H. M. A. Qahtani, et al., College Students Attributional Differences in Knowledge Awareness about a Cybercrimes Law. Journal of Ecohumanism. vol. 3, no. 6, pp. 773-786, 2024. doi: 10.62754/joe.v3i6.4046

[6] D. Mwiraria, K. Ngetich, and P. Mwaeke, Exploring individual factors associated with the prevalence of cybercrime victimization among students at Egerton University, Kenya. European Journal of Humanities and Social Sciences. vol. 4, no. 5, pp. 35-40, 2024. doi: 10.24018/ejsocial.2024.4.5.515

[7] N. A. Balogun, M. D. Abdulrahaman, and K. Aka, Exploring the prevalence of internet crimes among undergraduate students in a Nigerian University: A case study of the University of Ilorin. Nigerian Journal of Technology. vol. 43, no. 1, pp. 71-79, 2024. doi: 10.4314/njt.v43i1.10

[8] K. Lin, Y. Wu, I. Y. Sun, et al., Telecommunication and cyber fraud victimization among Chinese college students: An application of routine activity theory. Criminology & Criminal Justice. vol. 25, no. 3, pp. 717-735, 2025. doi: 10.1177/17488958221146144