Financial Economics Insights

Article

Research on Security Situation Awareness Model Based on Financial Industry Payment Scenario

Yingjie Ma [1,*]

[1] Wells Fargo Bank, N.A, Oxnard, 93030, California, USA
* Correspondence: Yingjie Ma, Wells Fargo Bank, N.A, Oxnard, 93030, California, USA

Abstract: With the rapid development of payment scenarios in the financial industry, cybersecurity threats are escalating, making payment systems a primary target for attackers. These systems face multiple challenges, including data breaches, fraudulent transactions, and malicious attacks. To address these issues, this paper proposes a cyber situational awareness model tailored to payment scenarios in the financial industry, aimed at enhancing the security capabilities of these systems. The model is designed with four layers: data acquisition, data processing, situational awareness, and response decision-making. It integrates multi-source data and applies machine learning algorithms for real-time analysis, achieving precise threat detection and effective response. Experimental results show that the model outperforms existing methods in detection accuracy, response speed, and applicability. It effectively identifies security vulnerabilities in payment systems and enables timely countermeasures. This study provides theoretical support and technical reference for security management in payment scenarios within the financial industry.

Keywords: financial industry; payment scenarios; cyber situational awareness; model design; cybersecurity

Published: 02 January 2025

1. Introduction

With the rapid advancement of digital technologies, payment scenarios in the financial industry are characterized by high-frequency transactions, real-time processing, and diverse services. However, these developments have also made payment systems a prime target for cyberattacks, posing significant threats such as data breaches, fraudulent transactions, and malicious software attacks. These security issues not only disrupt the stability of payment systems but also erode user trust and cause substantial financial losses. Therefore, effectively sensing and responding to security threats in payment scenarios has become a critical challenge for the financial industry. Cyber situational awareness (CSA) emerges as a promising technical approach for monitoring, analyzing, and assessing system security in real-time, offering new perspectives for security management in payment scenarios. By integrating multi-source data, analyzing potential threats, and generating actionable insights, CSA provides timely and comprehensive security information to decision-makers. However, most existing CSA models are designed for traditional IT systems and network environments, often falling short in addressing the unique demands of payment scenarios, such as transaction-specific features and the need for real-time threat detection and response. To overcome these limitations, this paper proposes a CSA model specifically tailored to payment scenarios in the financial industry. The model incorporates four layers—data acquisition, data processing, situational awareness, and response decision-making—to comprehensively address the security management needs of payment systems. By leveraging machine learning algorithms and multi-source data fusion techniques, the model enables real-time threat detection and delivers precise situational

assessments and response strategies. This research not only provides new ideas for managing payment system security but also lays a theoretical and practical foundation for related fields.

2. Related Research

2.1. Concept and Classification of Cyber Situational Awareness

With the rapid expansion of payment scenarios in the financial industry, characterized by high-frequency transactions, real-time processing, and multi-channel access, payment systems have become key targets for cyberattacks. These systems face multiple threats, including fraudulent transactions, data breaches, and malicious software attacks. The complexity of these security challenges has exposed the limitations of traditional static security methods, prompting researchers to adapt CSA theories and techniques to payment scenarios. The core objective of CSA is to achieve a comprehensive understanding of system security through multi-layered processes of perception, comprehension, and prediction. Following Endsley's theoretical framework, CSA can be divided into three key stages: Perception, which involves detecting the current state of the system; Comprehension, which provides a deeper understanding of the detected threats; and Prediction, which forecasts future risks. For payment scenarios, an additional stage—Mitigation—is often included to address threats dynamically, providing a full spectrum of threat management from detection to resolution.

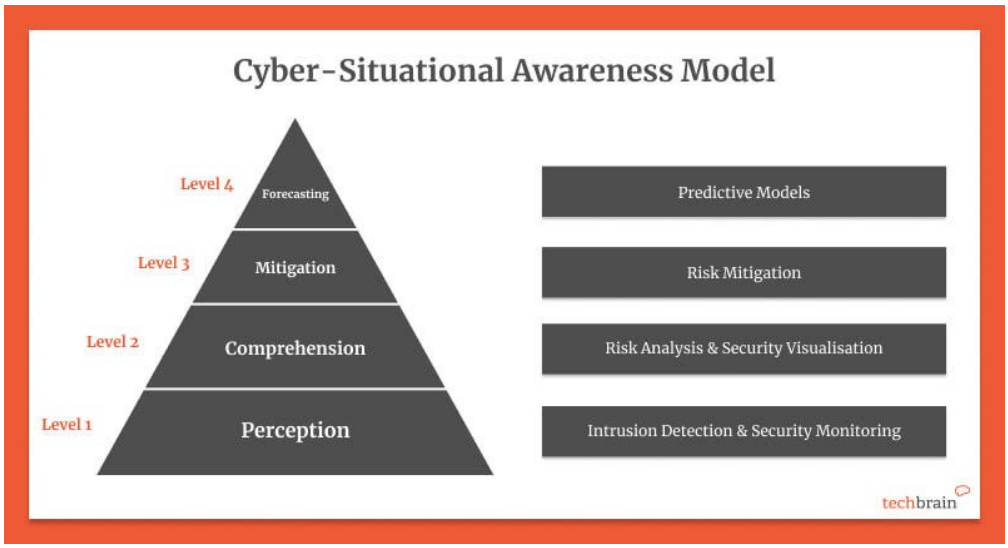

Figure 1. illustrates the architecture of the CSA model for payment scenarios in the financial industry.

As shown in Figure 1, the security situation awareness model based on payment scenarios in the financial industry can be divided into the following four levels:

1) Level 1: Perception

This foundational layer is responsible for real-time monitoring of security threats in payment systems. By collecting data from transaction logs, network traffic, system logs, and third-party threat intelligence, the model can swiftly identify potential threats, such as fraudulent transactions or abnormal payment requests. Techniques such as intrusion detection systems (IDS) and security monitoring tools are integrated at this layer to ensure baseline security.

2) Level 2: Comprehension

This layer further processes data from the perception layer, integrating payment business logic and risk rules to conduct risk analysis and security visualization. Beyond identifying individual threats, this layer assesses the scope and potential impact of threats

through correlation analysis. For instance, when abnormal traffic is detected in a specific payment channel, this layer evaluates whether the threat might propagate to other channels and provides actionable insights.

3) Level 3: Mitigation

The mitigation layer implements dynamic risk mitigation strategies to address threats identified by the comprehension layer. In payment scenarios, this includes automated decisions by risk control systems, such as dynamic adjustments to payment limits or freezing suspicious accounts. This layer also emphasizes collaboration with Security Operations Centers (SOCs) to rapidly block attack paths through human-machine coordination, minimizing the impact of security incidents on payment systems.

4) Level 4: Forecasting

Leveraging historical payment data and machine learning techniques, the forecasting layer builds predictive models to identify potential security threats in advance. This layer forecasts abnormal transaction patterns and emerging fraud trends, providing proactive security guidance. For example, it can predict peak periods for payment fraud in specific regions or timeframes, enabling managers to allocate resources in advance.

Compared to traditional IT systems, CSA models for payment scenarios demand higher levels of real-time performance, accuracy, and adaptability. Payment systems involve large volumes of rapidly changing transaction data, requiring efficient processing of high-frequency data streams with minimal latency. Researchers have integrated advanced techniques, such as distributed computing, real-time stream processing, and multi-source data fusion, into model design to meet these unique demands. In summary, the proposed CSA model for payment scenarios establishes comprehensive control over payment system threats through its four-layered architecture. Future research should explore optimization opportunities through emerging technologies, such as artificial intelligence, big data, and blockchain, to enhance the model's intelligence, real-time performance, and scalability in addressing increasingly complex security challenges [1].

2.2. Security Challenges in Payment Scenarios

The rapid digitization of the financial industry has introduced increasing complexity and diversity to payment scenarios, encompassing not only traditional bank transfers but also mobile payments, online shopping, and cross-border transactions. This complexity creates new vulnerabilities for cybercriminals, presenting unprecedented security challenges for payment systems. Figure 2 summarizes the key cybersecurity threats currently facing the financial payment sector, which span technical, organizational, and third-party risks [2].

Figure 2. Emerging Cybersecurity Threats in Financial Payment Scenarios.

Among these threats, third-party risk is particularly prominent. Payment systems often collaborate with external vendors, payment gateways, and fintech companies, which may serve as weak links in the security chain. A breach in these third-party systems can result in cascading effects, including data leaks and system outages across the entire payment ecosystem. Other significant threats include phishing attacks and malware, where attackers impersonate legitimate entities to deceive users into providing sensitive information, such as credit card numbers or account credentials. Malware infections on payment terminals can lead to data theft or unauthorized transaction modifications. Ransomware and DDoS attacks have more immediate impacts, disrupting the availability of payment systems. Ransomware encrypts system files to extort payment, while DDoS attacks overwhelm systems with traffic, rendering them inaccessible [3]. The rise of remote work has also intensified security challenges. Employees accessing critical payment systems from unsecured environments have increased vulnerability to attacks. Furthermore, AI-related threats are emerging, as attackers use AI to craft sophisticated phishing campaigns or identify system vulnerabilities more rapidly. Lastly, data breaches and Trojans/key loggers remain persistent threats, exposing sensitive user data and stealing critical transaction details. Addressing these challenges requires enhanced real-time threat monitoring, AI and big data analytics, stronger third-party security partnerships, and robust security strategies for remote work environments. Comprehensive CSA models can equip payment systems to effectively navigate these complex security landscapes, ensuring sustainable growth in the financial industry [4].

3. Model Design

3.1. Design Objectives and Principles

The design of a cyber situational awareness model for payment scenarios in the financial industry must fully account for the characteristics and security requirements of

payment systems. Payment scenarios involve high-frequency transactions, the transmission of large amounts of sensitive data, and diverse, complex security threats. Thus, the model should focus on real-time capabilities, accuracy, intelligence, and scalability, while also ensuring compatibility and operational effectiveness. One key objective is to achieve real-time system responsiveness. Given the millisecond-level response requirements of payment transactions, the model must rapidly detect and respond to threats, ensuring continuous control of the system's security status. Accuracy is another core goal, as the model must precisely identify and assess threat types, minimizing false positives and false negatives to reduce disruption to business operations. Intelligence is reflected in the model's ability to leverage artificial intelligence techniques to autonomously learn new threat patterns, dynamically adapt, and predict future risks. Scalability is crucial to accommodate the increasing volume and complexity of transactions as payment systems grow [5]. Additionally, compatibility ensures the model can seamlessly integrate with existing payment system architectures and security tools. From a design principles perspective, a layered structure is the core approach. By dividing the model into four levels—Perception, Comprehension, Mitigation, and Prediction—each level can focus on specific functions while collaborating to provide comprehensive threat management. Multi-source data fusion is a key enabler for the model's efficiency, combining transaction logs, network traffic, user behavior data, and external threat intelligence to deliver a holistic security view. The principle of risk minimization emphasizes prioritizing high-risk threats to safeguard critical payment operations. Dynamic adaptability ensures the model can adjust detection strategies and response measures in real-time as threats evolve. Lastly, explain ability is essential, enabling the model to produce clear and interpretable threat analysis results that security teams can quickly understand and act upon [6]. The table 1 below summarizes the alignment between design objectives and principles:

Table 1. Correspondence between design goals and principles of the model.

Design Objective	Implementation Principle	Description
Real-time system responsiveness	Layered structure, dynamic adaptability	Enhances threat detection and response speed through modular design.
Improved threat detection accuracy	Multi-source data fusion, risk minimization	Analyzes threat characteristics using diverse data sources and prioritizes critical threats.
Business scalability	Layered structure, dynamic adaptability	Modular design and flexible strategies support seamless expansion for growing demands.
Enhanced intelligence	Dynamic adaptability, multi-source data fusion	Employs AI to strengthen the identification and prediction of unknown threats, achieving higher automation levels.
Ensured system compatibility	Layered structure, explain ability	Integrates with existing payment systems and provides clear threat analysis outputs for easy operation.

With these objectives and principles, the cyber situational awareness model effectively addresses the diverse and complex security threats in payment scenarios, providing comprehensive protection while improving system security and stability [7].

3.2. Model Architecture

In payment scenarios, the architecture of the cyber situational awareness model must cover the entire lifecycle, from threat detection to response decision-making, and dynamically adapt to environmental changes. Figure 3 presents a systematic model architecture

based on situational awareness theory, which integrates environmental conditions, information processing mechanisms, and decision-making processes into a layered and adaptive security management framework [8].

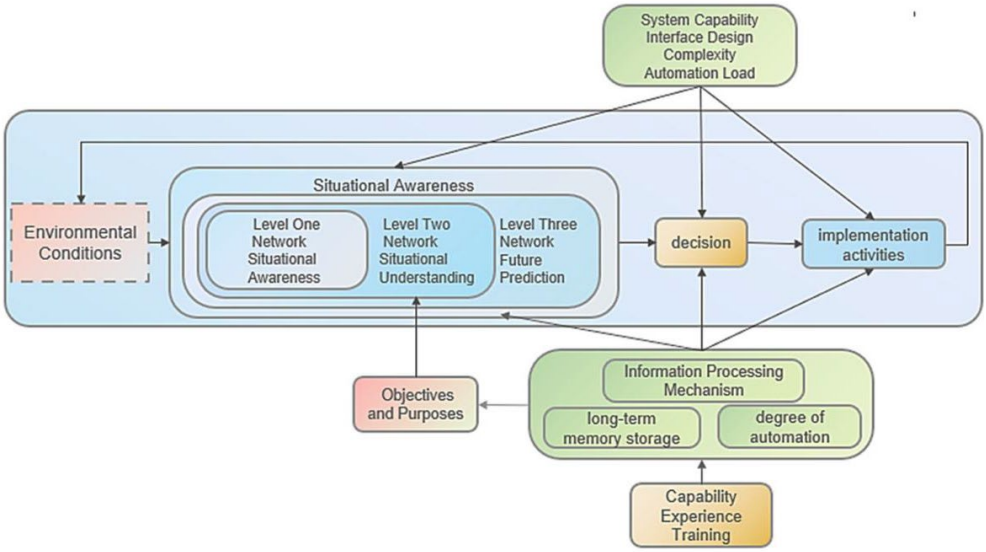

Figure 3. Cyber Situational Awareness Model Architecture for Payment Scenarios.

The core of the model consists of three levels of cyber situational awareness: Level One: Network Situational Awareness, This level focuses on real-time perception of key threats and security events in the environment. By integrating payment transaction logs, network traffic data, and threat intelligence, it rapidly identifies anomalies or potential threats. Level Two: Network Situational Understanding, Based on raw data provided by the perception layer, this level uses risk analysis and data correlation techniques to deeply analyze the nature, scope, and potential impact of threats. In payment scenarios, this level identifies fraudulent transaction chains or behaviors that may lead to systemic risks. Level Three: Network Future Prediction, the prediction layer leverages machine learning algorithms and historical data to anticipate future security events. This layer provides forward-looking support for payment system security, such as forecasting DDoS attacks during peak transaction periods or identifying the spread of new phishing techniques. The model's operation is influenced by multiple external and internal factors. Environmental conditions, including transaction environments, user behaviors, and third-party networks, serve as inputs for the model. These conditions are processed by an information processing mechanism that includes long-term memory storage and degrees of automation to ensure the efficiency and accuracy of the processing results. The decision module is a critical component of the model, responsible for formulating response strategies based on the situational analysis results [9]. For payment scenarios, the decision module must be both flexible and precise, capable of initiating payment freezes, risk alerts, and strategy adjustments. Finally, the decisions are translated into implementation activities, such as intercepting malicious payment requests or adjusting transaction limits. Additionally, the model emphasizes system capability, including interface design, complexity, and automation load. The model's effectiveness not only relies on data processing and decision-making mechanisms but also requires capability-building and training to enhance overall security performance. For example, improving the skills of security teams and optimizing payment system processes can significantly boost the model's performance in practical applications. Through this architecture design, the model comprehensively addresses the complex security threats in payment scenarios. It not only detects current threats in real-

time but also provides forward-looking support through predictive capabilities, creating a dynamic and adaptive security management system for payment systems [10].

4. Data Processing and Analysis

4.1. Data Sources and Preprocessing

In the cyber situational awareness model for financial payment scenarios, data sources form the foundational basis for model design. The data in payment scenarios is complex and diverse, encompassing transaction behavior, network traffic, system logs, and external threat intelligence. These data sources are characterized by real-time, high-frequency attributes, but may also contain inconsistencies and noise, making effective preprocessing essential to ensure data quality and consistency. To fully support the model's functionality, the data sources are divided into the following categories: Payment Transaction Logs: These logs record detailed information about each transaction, including transaction amount, timestamp, user ID, and payment channel. This data is crucial for identifying anomalous transactions. Network Traffic Data: This includes network communication data within the payment system, such as IP addresses, access frequencies, and packet contents, which help detect potential network attacks. System Logs: These logs, including server operation logs and error logs, assist in monitoring system status and identifying malicious activities or potential threats. External Threat Intelligence: This consists of threat information from third-party security providers or open-source threat intelligence platforms, including the latest attack patterns and lists of malicious IP addresses. User Behavior Data: This tracks user payment operations, such as device usage, geographic location, and payment habits, which are used to build user behavior models. The table 2 below provides an overview of the main fields for each data source:

Table 2. Data Source.

Data Source	Field Names	Description
Payment Transaction Logs	Transaction ID, User ID, Amount, Timestamp	Basic information for each payment transaction.
Network Traffic Data	Source IP, Destination IP, Packet Size, Access Frequency	Key characteristics of network communication behavior.
System Logs	Timestamp, Log Type, Event Description	Records the system's operational state and exceptions.
External Threat Intelligence	Malicious IP Addresses, Attack Types, Risk Levels	Provides real-time information on known threats.
User Behavior Data	User ID, Device Type, Geographic Location, Payment Habits	Describes user operations and preferences.

Given the complexity and diversity of data sources, the following preprocessing steps are necessary to ensure the model's accuracy and stability: Data Cleaning: Remove null values, incomplete data, and anomalies, such as invalid network packets and invalid transactions in payment logs. Data Formatting: Standardize field names and formats, such as aligning timestamp formats across different sources to facilitate data integration. Data Denoising: Apply filtering and dimensionality reduction techniques to remove redundant information and high-frequency noise in network traffic, ensuring data reliability. Data Augmentation: Enrich user behavior data with contextual information, such as combining historical transaction data to enhance payment behavior features. Feature Extraction: Extract key features from raw data, such as statistical characteristics of transaction amounts, spectral features of network traffic, and temporal patterns of user behavior, to support subsequent analysis and modeling. By leveraging high-quality data sources and systematic preprocessing methods, the situational awareness model can obtain accurate and comprehensive input data. These data support the model's capabilities in threat detection

and analysis, while also laying a robust foundation for risk prediction and dynamic response.

4.2. Key Techniques and Algorithms

In the situational awareness model for financial payment scenarios, algorithmic techniques are the driving force behind effective threat perception, analysis, and prediction. By employing advanced machine learning and data mining techniques, the model can efficiently handle complex, multi-source data and deliver robust performance in real-time detection, risk evaluation, and threat prediction. This section introduces the key technical methods and core algorithms that meet the model's requirements.

4.2.1. Multi-Class Threat Detection Algorithm

Payment scenarios involve multiple types of threats, including fraudulent transactions, malware attacks, and abnormal network traffic. To identify these threats, multi-class algorithms such as Support Vector Machines (SVM) can be used. The multi-class objective can be expressed as shown in Formula 1:

$$f(x) = \arg\max_k(w_k \cdot x + b_k) \quad (1)$$

where $f(x)$ is the classification decision function, k denotes the threat category (e.g., fraudulent transactions or normal transactions), w_k and b_k are the classifier's weights and biases, respectively, and x is the input feature vector (e.g., transaction amount or time intervals). SVM maximizes the classification margin to improve accuracy.

4.2.2. Time Series Prediction Algorithm

To forecast future threats in payment systems, Long Short-Term Memory (LSTM) networks can be employed for time series prediction. LSTM effectively captures temporal dependencies in payment data to predict potential attack trends or abnormal transactions. The LSTM cell update formula is as shown in Formula 2:

$$h_t = o_t \odot \tanh(c_t) \quad (2)$$

where h_t is the hidden state at time t, o_t is the output gate, c_t is the cell state, and $\odot$ represents element-wise multiplication. Through recursive computations, LSTM learns historical behavioral patterns in payment systems and predicts future threats.

4.2.3. Data Clustering Algorithm

In large-scale payment data, some anomalous transactions may not be labeled. To uncover these potential threats, K-Means Clustering, an unsupervised learning method, can be applied. By clustering, transaction data can be grouped into different categories, and anomalies can be identified as outliers. The K-Means objective function is as shown in Formula 3:

$$J = \sum_{i=1}^{K} \sum_{x \in C_i} \| x - \mu_i \|^2 \quad (3)$$

where K is the number of clusters, C_i represents the i-th cluster, μ is the centroid of cluster C_i, and x is a data point. Minimizing J groups similar transactions while segregating anomalies into distinct clusters. These three algorithms play distinct roles within the model: Multi-Class Threat Detection identifies known threat categories in real-time, making it suitable for rapid response in payment scenarios. Time Series Prediction enables dynamic early warning systems for future threats, providing proactive decision-making support for managers. Data Clustering Analysis uncovers unknown threats, contributing to the model's continuous optimization and extension. By integrating these algorithms, the model achieves comprehensive capabilities, ranging from static detection to dynamic prediction, providing efficient and intelligent security protection for financial payment scenarios.

5. Experiment and Validation

To evaluate the effectiveness of the cyber situational awareness model tailored for financial payment scenarios, a series of experiments were designed and conducted to assess the model's performance in threat detection, risk analysis, and situational forecasting. The experimental data comprised real payment system logs, simulated network traffic data, and external data from third-party threat intelligence platforms. The focus was on evaluating the model's accuracy, real-time responsiveness, and predictive capabilities. The goal of the experiments was to thoroughly assess the practical performance of the model across three main tasks: threat detection, risk analysis, and threat prediction. To achieve this, the experiment was divided into three stages: data preparation, experimental setup, and performance evaluation.

Table 2. Experimental Data.

Data Source	Sample Size	Key Features	Objective
Payment Transaction Logs	500,000	Transaction amount, timestamp, user ID	Anomalous transaction detection
Network Traffic Data	100,000	Source IP, destination IP, packet size	Anomalous network traffic detection
External Threat Intelligence	10,000	Malicious IPs, attack patterns	Threat feature extraction and analysis

As shown in Table 2, the dataset used in the experiments consisted of three components, covering critical data sources in payment scenarios. First, payment transaction logs formed the core of the dataset, containing approximately 500,000 transaction records with attributes such as transaction amount, timestamp, user ID, and payment channel. These logs provided the basis for anomaly detection. Second, network traffic data, consisting of 100,000 communication records with features such as source IP, destination IP, packet size, and communication frequency, was used to capture potential network threats in the payment system. Finally, external threat intelligence from third-party platforms included 10,000 malicious IPs and known attack patterns, enriching the model's ability to identify new threats. To ensure data quality and consistency, several preprocessing steps were applied to the raw data. Data cleaning removed invalid or incomplete records, while denoising eliminated redundant information from network traffic. Additionally, feature extraction identified key variables such as transaction amount distributions, user behavior patterns, and network traffic characteristics, ensuring high-quality input for model training and testing. The experimental setup involved three specific tasks: Threat Detection: Support Vector Machines (SVM) were used to classify anomalous transactions in payment logs, aiming to evaluate the model's ability to identify known threats. Risk Analysis: K-means clustering was employed to group unlabelled data and uncover potential unknown threats. Threat Prediction: Long Short-Term Memory (LSTM) networks were utilized to predict abnormal transaction trends within the next hour, providing forward-looking security recommendations for the payment system. The experiments evaluated the model's performance using four key metrics: Accuracy: Measures the overall correctness of the model in threat detection. Recall: Reflects the model's sensitivity in identifying anomalous transactions. Response Time: Assesses the model's real-time performance in payment scenarios. Prediction Error: Evaluates the accuracy of the LSTM model in the threat prediction task. These stages provided a robust foundation for comprehensively assessing the model's functionality. The results revealed the model's applicability and areas for improvement in real-world payment scenarios. As illustrated in Figure 4, the SVM classification model performed effectively in detecting threats within payment transaction logs.

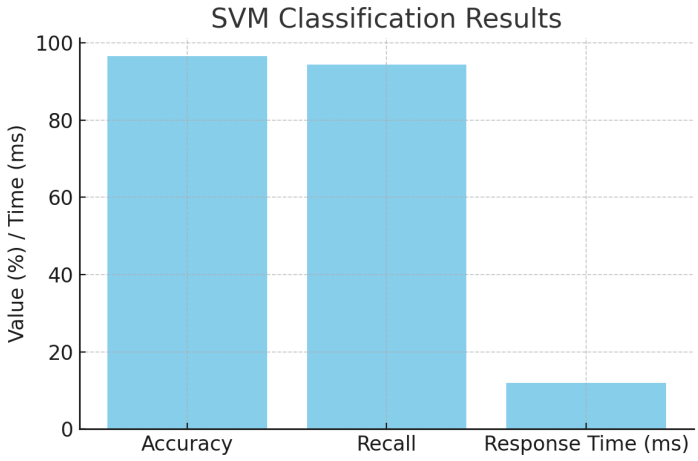

Figure 4. SVM Classification Results.

The results demonstrated high accuracy and recall rates, effectively identifying anomalous transactions in payment scenarios. Additionally, the response time met the real-time requirements of payment systems. Figure 5 shows the results of K-means clustering on network traffic data.

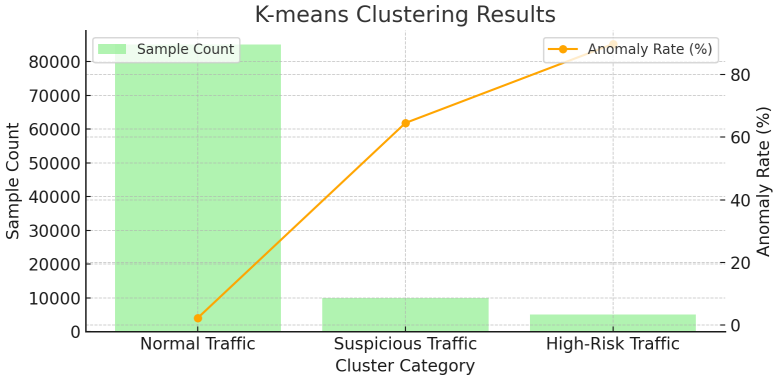

Figure 5. K-means Clustering Results.

The clustering method effectively distinguished normal traffic from anomalous traffic, with an anomaly rate of nearly 90% for high-risk traffic, demonstrating strong anomaly detection capabilities. The performance of the LSTM model in predicting abnormal transactions for the next hour is shown in Figure 6.

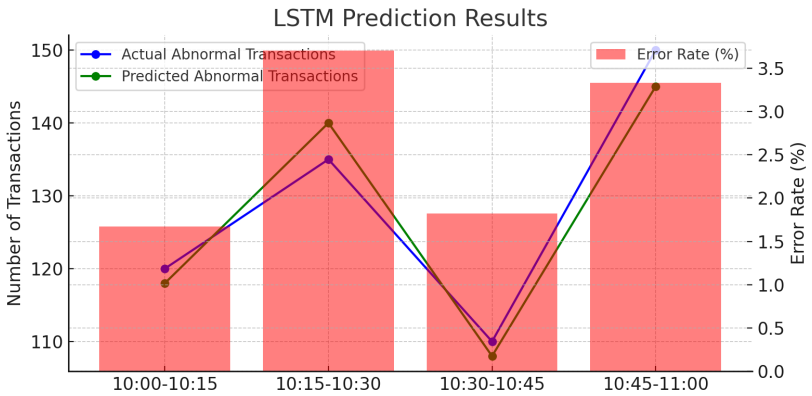

Figure 6. LSTM Prediction Results.

The results indicated that the LSTM model accurately predicted future abnormal transaction trends, with a prediction error rate consistently below 5%. Overall, the experimental results confirmed the model's excellence in threat detection, risk analysis, and future trend prediction. The application of the model in payment scenarios significantly improved the ability to identify anomalous transactions and predict system risks, providing robust support for the security of financial payment systems. Additionally, the results validated the model's real-time efficiency and effectiveness, demonstrating its feasibility and practicality in real-world scenarios.

6. Conclusion

This paper proposed a cyber situational awareness model tailored for financial payment scenarios, achieving comprehensive protection against complex security threats through four layers: perception, comprehension, mitigation, and prediction. Experimental results demonstrated the model's outstanding performance in detection accuracy, in-depth risk analysis, and forward-looking predictive capabilities, meeting the high requirements of real-time security in payment systems. The model's integration of multi-source data and intelligent algorithms also provided strong support for its scalability and adaptability in practical applications. Future research will focus on optimizing the model's algorithmic efficiency and incorporating emerging technologies such as blockchain and privacy-preserving computation to further enhance its security performance and application scope.

References

1. Ahmad, A., et al., "How can organizations develop situation awareness for incident response: A case study of management practice," *Comput. Secur.*, vol. 101, p. 102122, 2021.
2. Y. Chen, E. K. Kumara, and V. Sivakumar, "Investigation of finance industry on risk awareness model and digital economic growth," *Ann. Oper. Res.*, pp. 1–22, 2021.
3. S. Varga, J. Brynielsson, and U. Franke, "Cyber-threat perception and risk management in the Swedish financial sector," *Comput. Secur.*, vol. 105, p. 102239, 2021.
4. Y. Liu and S. Zhu, "Multimodal wireless situational awareness-based tourism service scene," *J. Sens.*, vol. 2021, no. 1, p. 5503333, 2021.
5. D. Bunker, "Who do you trust? The digital destruction of shared situational awareness and the COVID-19 infodemic," *Int. J. Inf. Manage.*, vol. 55, p. 102201, 2020.
6. Z. Li, et al., "Situation-aware multivariate time series anomaly detection through active learning and contrast VAE-based models in large distributed systems," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 9, pp. 2746–2765, 2022.
7. R. Riesco, X. Larriva-Novo, and V. A. Villagrá, "Cybersecurity threat intelligence knowledge exchange based on blockchain: Proposal of a new incentive model based on blockchain and smart contracts to foster the cyber threat and risk intelligence exchange of information," *Telecommun. Syst.*, vol. 73, no. 2, pp. 259–288, 2020.
8. M. Gazzan and F. T. Sheldon, "Opportunities for early detection and prediction of ransomware attacks against industrial control systems," *Future Internet*, vol. 15, no. 4, p. 144, 2023.
9. C. Calliess and A. Baumgarten, "Cybersecurity in the EU the example of the financial sector: A legal perspective," *Ger. Law J.*, vol. 21, no. 6, pp. 1149–1179, 2020.
10. Z. Liu and L. Wang, "FlipIt game model-based defense strategy against cyberattacks on SCADA systems considering insider assistance," *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 2791–2804, 2021.