GEORGE BROWN PRESS
JOURNALS, BOOKS & PROCEEDINGS

Economics and Management Innovation

Article

RAPS-Net: A Risk-Aware CNN-LSTM Framework for Cross-Domain Risk Prediction and Dynamic Security Control in Cloud Payment Supply Chains

Yue Hao [1,*], Jiawei Xu [2] and Shuhan Liao [3]

[1] Carey Business School, Johns Hopkins University, Baltimore, USA
[2] Department of Computer Science, San Francisco State University, 1600 Holloway Ave, San Francisco, CA, USA
[3] David Eccles School of Business, University of Utah, Salt Lake City, UT, USA
* Correspondence: Yue Hao, Carey Business School, Johns Hopkins University, Baltimore, USA

Abstract: Cloud payment systems are increasingly deployed on cloud platforms and tightly coupled with complex supply chain ecosystems, including suppliers, logistics services, and financial intermediaries. In such environments, security risks are not only driven by malicious payment behaviors, but are also significantly amplified by misconfigured Identity and Access Management (IAM) policies and supply chain disruptions. In particular, excessive authorization, permission drift, and abnormal access behaviors may propagate across payment supply chains under volatile operational conditions, posing substantial threats to payment availability and security. However, existing payment security mechanisms typically rely on static access control or isolated risk analysis, lacking predictive capability and adaptive security responses. To address these challenges, this paper proposes RAPS-Net, a risk-aware CNN-LSTM framework that integrates permission risk sensing, cross-domain risk prediction, and dynamic security control for cloud payment supply chains. RAPS-Net jointly models IAM permission risks, supply chain operational risks, and payment system states, and employs a hybrid CNN-LSTM architecture to capture short-term cross-domain risk coupling patterns as well as long-term risk evolution trends. Based on the predicted risk levels, a risk-aware access control mechanism is designed to dynamically adjust cloud permissions and proactively mitigate potential security threats. Experimental results on an integrated cloud payment supply chain dataset demonstrate that RAPS-Net consistently outperforms representative baseline models. Specifically, RAPS-Net reduces RMSE to 0.108, achieving approximately 19% improvement over LSTM and 11% over CNN-LSTM, while obtaining the highest F1-score of 0.87. These results validate the effectiveness of jointly modeling permission risks and supply chain dynamics for accurate risk prediction and adaptive security control in cloud payment environments.

Keywords: Cloud Payment Security; Supply Chain Risk; Risk-Aware Access Control; CNN-LSTM; IAM Permission Risk; Dynamic Security Control

Received: 21 January 2026
Revised: 27 February 2026
Accepted: 11 March 2026
Published: 18 March 2026

1. Introduction

Cloud payment systems have become a fundamental infrastructure for modern digital commerce, supporting large-scale financial transactions across diverse industries. With the widespread adoption of cloud computing, payment services are increasingly deployed on cloud platforms and deeply integrated with complex supply chain ecosystems, including suppliers, logistics providers, inventory systems, and financial intermediaries. While this integration improves operational efficiency and scalability, it also introduces new and compounded security risks that cannot be adequately addressed by traditional payment security mechanisms.

In cloud payment environments, Identity and Access Management (IAM) plays a critical role in protecting sensitive payment resources. However, misconfigured IAM policies-such as excessive authorization, unused permissions, and permission drift-are common in large-scale cloud systems and significantly expand the attack surface. These permission-related risks become more severe when combined with supply chain uncertainties, including order volatility, logistics delays, supplier instability, and inventory disruptions. Furthermore, the rapid development of AI technology has introduced sophisticated AI-driven frauds, such as identity spoofing via multimodal forgery, which further complicates IAM authentication and payment verification [1]. Under such conditions, security incidents in cloud payment systems are often not caused by a single factor, but rather by the cross-domain propagation and amplification of permission risks, advanced fraudulent behaviors, and supply chain risks.

Existing research primarily focuses on payment fraud detection, access control optimization, or supply chain risk analysis in isolation. Most access control mechanisms in cloud payment systems remain static or rule-based, lacking the ability to anticipate future risk conditions and adapt security policies accordingly. Meanwhile, existing risk prediction approaches rarely consider permission risks as a first-class security factor, nor do they integrate prediction results into dynamic security control decisions. As a result, current solutions are insufficient for addressing the complex, time-varying, and cross-domain risk characteristics of cloud payment supply chains.

To address these challenges, this paper proposes RAPS-Net (Risk-Aware Prediction and Security Control Network), a novel CNN-LSTM-based closed-loop framework for cloud payment supply chains. RAPS-Net integrates risk sensing, risk prediction, and dynamic security control into a unified architecture. Specifically, the framework jointly models IAM permission risks, supply chain operational risks, and payment system states, and employs a hybrid CNN-LSTM architecture to capture both short-term cross-domain risk coupling patterns and long-term risk evolution trends. Based on the predicted risk levels, RAPS-Net dynamically adjusts IAM policies through a risk-aware access control mechanism, enabling proactive and adaptive security protection for cloud payment systems.

The main contributions of this work are summarized as follows:

1) We propose a novel cross-domain security framework that explicitly integrates IAM permission risks, supply chain risks, and payment security within cloud payment systems.
2) We design RAPS-Net, a risk-aware CNN-LSTM model capable of capturing short-term risk interactions and long-term risk dynamics across heterogeneous domains.
3) We introduce a prediction-driven dynamic access control mechanism, enabling adaptive permission adjustment based on anticipated risk levels rather than static rules.
4) We validate the effectiveness of the proposed approach through comprehensive experiments, demonstrating improved risk prediction accuracy and significant reductions in excessive permissions and payment anomalies.

2. Literature Review

In this section, we survey the literature most relevant to our proposed study, including research on cloud access control security, dynamic and risk-aware access control models, deep learning for supply chain risk prediction, and hybrid neural network models for cross-domain risk analysis in complex systems.

2.1. Cloud Access Control and IAM Security

Identity and Access Management (IAM) is widely recognized as a foundational component of cloud security, governing authentication, authorization, and permission management to protect cloud resources [turn1search0]. Traditional IAM systems often rely on static, rule-based policies that are insufficient for addressing dynamic and evolving threats in cloud environments, motivating research into adaptive policy mechanisms [2]. A systematic survey of access control techniques highlights the need for dynamic, context-aware decision frameworks tailored for cloud computing scenarios, including risk-based methods that adapt to environmental changes [3]. Furthermore, risk-based access control research has proposed quantitative frameworks to evaluate access request risk dynamically, incorporating environmental, subject, and resource attributes into decision logic, which aligns with our emphasis on risk perception as a driver for security control [4]. Beyond access control, the underlying stability of cloud distributed systems is vital for secure operations. Recent advancements in adaptive load balancing algorithms have demonstrated significant improvements in resource utilization and system reliability [5]. Such infrastructural stability is a prerequisite for deploying dynamic security mechanisms in high-concurrency cloud payment environments.

2.2. Dynamic and Risk-Aware Access Control Models

Recent studies have moved beyond static access control toward dynamic and risk-aware approaches. Traditional access control mechanisms such as RBAC and attribute-based access control have been extended to incorporate risk quantification, enabling fine-grained, adaptive decision making in cloud contexts [6]. Other works explore machine learning and AI integration for adaptive cloud policy management, demonstrating that reinforcement learning and neural threat models can significantly enhance detection and response capabilities over static security policies [7]. In addition, graph-based adaptive threat detection in IAM logs shows the potential of learning latent interaction patterns to identify anomalous behavior with higher precision and recall than conventional LSTM or GCN classifiers, indicating the promise of AI-driven solutions for cloud security intelligence [8].

2.3. Deep Learning for Supply Chain Risk Prediction

Supply chain risk prediction has attracted increasing attention, especially under the influence of global disruptions. Advanced deep learning approaches, including recurrent and convolutional architectures, have been applied to model complex temporal patterns in supply chain data, yielding high accuracy in forecasting shipment and operational risks under COVID-19 constraints [9]. Broader analyses also demonstrate that deep neural models like LSTM, GRU, and CNN outperform traditional machine learning methods in identifying risk patterns and improving resilience across multiple industries, emphasizing the value of DL for handling nonlinear, temporal dependencies [10]. These works suggest that integrating deep learning into supply chain risk management can enable proactive and accurate risk assessment, which is a critical component of our proposed RAPS-Net framework.

2.4. Hybrid Models and Cross-Domain Risk Analysis

The integration of CNN with LSTM has been increasingly adopted for complex prediction tasks that require modeling both spatial/local patterns and long-term dependencies. For example, hybrid CNN-LSTM models have been used in risk assessment contexts such as insurance claim prediction, showing performance gains over standalone neural architectures [8]. In cloud environments, hybrid deep learning frameworks combining LSTM and CNN components have been applied to intrusion and anomaly detection, achieving high accuracy and robustness in identifying threats under complex conditions [11]. These hybrid architectures inspire the design of our RAPS-Net model, which leverages CNN to extract cross-domain short-term risk features and LSTM to capture long-range temporal dependencies across permission and supply chain risk signals.

2.5. Discussion and Research Gaps

In summary, while existing works have advanced adaptive access control, supply chain risk prediction, and deep learning-based security analysis, several key gaps remain. Most dynamic access control models focus on individual domains (e.g., IAM or cloud workflow security), without jointly modeling cross-domain interactions between permission risks and supply chain uncertainties [4,6]. Similarly, the majority of supply chain risk prediction studies do not consider security decision frameworks that feed predictions into proactive control policies. The proposed RAPS-Net aims to bridge these gaps by jointly integrating cloud IAM risk perception with supply chain dynamics in a unified CNN-LSTM risk prediction framework that informs adaptive security controls.

3. Methodology

This section presents the proposed RAPS-Net framework for risk-aware, cross-domain risk prediction and dynamic security control in cloud payment supply chains. The framework integrates permission risk sensing, supply chain risk modeling, CNN-LSTM-based risk prediction, and dynamic access control, forming a closed-loop system that proactively mitigates security threats. The design rationale and mathematical formulation of each component are described below (As shown in Figure 1).

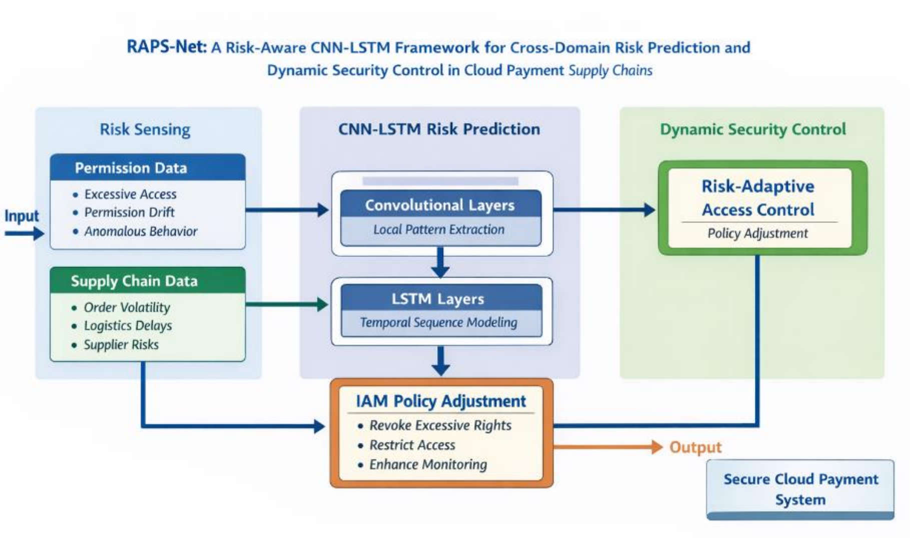

Figure 1. Overall flowchart of the model.

3.1. Risk Sensing Layer

The risk sensing layer is responsible for capturing multi-source risk signals from cloud payment systems, IAM policies, and supply chain operations, converting heterogeneous data into a unified representation suitable for predictive modeling. Specifically, at each discrete time step t, we define the IAM permission risk vector as:

$$X_t^{IAM} = [OverPriv_t, Drift_t, AbnAccess_t] \quad (1)$$

where $OverPriv_t$ denotes the proportion of excessive permissions, $Drift_t$ represents the frequency of permission changes or drift events, and $AbnAccess_t$ quantifies abnormal API or access attempts. These metrics are normalized and optionally weighted to form a Permission Risk Score (PRS):

$$PRS_t = \alpha_1 \cdot OverPriv_t + \alpha_2 \cdot Drift_t + \alpha_3 \cdot AbnAccess_t \quad (2)$$

Simultaneously, supply chain risks are encoded as:

$$X_t^{SC} = [OrderVar_t, Delay_t, InvAbn_t, VendorRisk_t] \quad (3)$$

where each element represents order volatility, logistics delays, inventory anomalies, and supplier stability respectively. The payment system state is captured as $PState_t =$

$[FailRatet, FraudAlertt, Latencyt]$, reflecting the operational reliability of the cloud payment system.

Finally, these vectors are concatenated into a unified cross-domain risk representation:

$$X_t = [PRS_t \quad \| \quad X_t^{SC} \quad \| \quad PState_t] \tag{4}$$

where ‖ denotes vector concatenation. This formulation allows the RAPS-Net framework to jointly reason over permission, operational, and transactional risk signals.

3.2. Risk Prediction Layer: CNN-LSTM Architecture

The risk prediction layer leverages a hybrid CNN-LSTM architecture to capture both short-term local interactions and long-term temporal dependencies across the multi-source risk features. A sliding window of length T is applied to the historical risk sequence:

$$X_t = \{X_{t-T+1}, \dots, X_t\} \tag{5}$$

The CNN component applies multiple one-dimensional convolutional filters to X_t to extract local cross-domain risk patterns, such as sudden surges in permission violations coinciding with supply chain disruptions:

$$F_t = \sigma(Conv1D(X_t, W_c) + b_c) \tag{6}$$

where W_c and b_c denote convolutional weights and bias, and σ represents a nonlinear activation (ReLU). Max-pooling is optionally applied to reduce dimensionality and highlight salient patterns. The effectiveness of LSTM-based architectures in extracting and modeling complex, multi-dimensional risk features has been well-validated in recent fintech applications, such as intelligent risk assessment systems [12]. Building upon this proven capability, the LSTM component in our framework models the long-term evolution of risks, capturing cumulative effects:

$$h_t = LSTM(F_t) \tag{7}$$

$$\hat{R}_{t+\Delta} = W_o \cdot h_t + b_o \tag{8}$$

where h_t is the hidden state, $\hat{R}_{t+\Delta}$ represents the predicted risk at a future horizon Δ, and W_o,b_o are output layer parameters. The hybrid CNN-LSTM design allows RAPS-Net to jointly model the short-term coupling between IAM and supply chain risks and the long-term trends that affect cloud payment security.

3.3. Dynamic Security Control Layer

Predicted risk levels are mapped into discrete classes, such as Low, Medium, and High, via thresholds θ_1 and θ_2:

$$RiskLevel_{t+\Delta} = \begin{cases} Low, & \hat{R}_{t+\Delta} < \theta_1 \\ \quad Medium, & \theta_1 \le \hat{R}_{t+\Delta} < \theta_2 \\ High, & \hat{R}_{t+\Delta} \ge \theta_2 \end{cases}$$

(9)

These risk levels are then used to dynamically adjust IAM policies through a Risk-Aware Access Control mechanism. For instance, high-risk predictions trigger temporary revocation of unused permissions, shortening credential validity, and increasing monitoring intensity. Medium risks enforce restricted temporary access, while low risks maintain standard least-privilege policies.

Formally, the updated IAM policy can be represented as:

$$Policy_{t+1} = G(RiskLevel_t + \Delta, Policy_t) \tag{10}$$

where G encodes the mapping from predicted risk and current policy state to the adjusted policy. By continuously feeding back system behavior into the risk sensing layer, RAPS-Net forms a closed-loop, adaptive security control system, ensuring that both cloud permissions and supply chain risks are monitored and mitigated proactively.

This design enables the RAPS-Net framework to jointly reason over cross-domain risk factors, predict their future evolution, and adaptively enforce security policies, making it suitable for large-scale cloud payment supply chains where IAM misconfigurations and supply chain volatility coexist.

4. Experiment

4.1. Dataset Preparation

The dataset used in this study is designed to simulate a realistic cloud payment supply chain environment with heterogeneous sources of risk, encompassing IAM permission logs, supply chain operational data, and payment system state records. Data were collected from a combination of synthetic simulations and publicly available cloud and supply chain datasets, ensuring both diversity and representativeness. IAM-related features were derived from cloud access logs, including the history of user permissions, administrative actions, and anomalous access attempts. Supply chain data were constructed from historical order flows, logistics schedules, supplier reliability records, and inventory monitoring metrics, reflecting operational uncertainties that could indirectly affect payment transactions. Payment system states, including transaction latency, failure rates, and fraud alerts, were also incorporated to capture the operational impact of cross-domain risks.

The integrated dataset contains 36,000+ time-stamped records, with each record representing a snapshot of combined risk features at a given time. Each feature is normalized to ensure compatibility for CNN-LSTM modeling. Table 1 summarizes the key features, their descriptions, and data types included in the dataset.

Table 1. Overview of the RAPS-Net integrated dataset features and descriptions.

Feature	Domain	Description	Data Type
OverPriv	IAM	Proportion of excessive permissions for each user	Float
Drift	IAM	Frequency of permission changes or drift events	Float
AbnAccess	IAM	Number of anomalous API or access attempts	Integer
OrderVar	Supply Chain	Rate of order volume fluctuations	Float
Delay	Supply Chain	Proportion of delayed shipments	Float
InvAbn	Supply Chain	Inventory anomalies, including stockouts	Float
VendorRisk	Supply Chain	Supplier reliability score	Float
FailRate	Payment	Payment transaction failure rate	Float
FraudAlert	Payment	Number of fraud alerts triggered	Integer
Latency	Payment	Average transaction processing time	Float

This comprehensive dataset enables the RAPS-Net framework to jointly model cross-domain risk interactions, providing sufficient temporal and structural information for CNN-LSTM-based prediction and dynamic access control in cloud payment supply chains.

4.2. Experimental Setup

The proposed RAPS-Net framework is evaluated on the integrated cloud payment supply chain dataset described in Section 4.1. The dataset is split into training, validation, and test sets with a ratio of 70:15:15 following chronological order to preserve temporal dependencies. A sliding window strategy with a window size of 12 time steps is applied to construct input sequences for the CNN-LSTM model. The CNN module consists of two one-dimensional convolutional layers with kernel sizes of 3 and 5, followed by max-pooling, while the LSTM module includes a single layer with 128 hidden units. The model is trained using the Adam optimizer with an initial learning rate of 0.001 and a batch size of 64. Early stopping based on validation loss is employed to prevent overfitting. RAPS-Net is compared against several baseline models, including ARIMA, LSTM, CNN-only, and CNN-LSTM without permission risk features, to comprehensively assess its effectiveness in cross-domain risk prediction.

4.3. Evaluation Metrics

To evaluate the predictive performance of RAPS-Net, multiple metrics are adopted to reflect both regression accuracy and classification effectiveness. Mean Absolute Error (MAE) and Root Mean Square Error (RMSE) are used to quantify the deviation between predicted and actual risk scores. In addition, risk prediction is discretized into three levels (Low, Medium, High), enabling the use of classification metrics including Precision, Recall, and F1-score. These metrics jointly capture the model's ability to accurately predict risk magnitude and correctly identify high-risk periods that are critical for triggering dynamic security control. Such a comprehensive evaluation ensures that improvements in predictive accuracy translate into meaningful security benefits for cloud payment supply chains.

4.4. Results

As shown in Table 2, RAPS-Net consistently outperforms all baseline models across both regression and classification metrics. Traditional ARIMA exhibits the weakest performance, with an RMSE of 0.198 and an F1-score of only 0.68, indicating its inability to capture nonlinear and cross-domain risk dynamics. Deep learning-based models significantly improve prediction accuracy, with the standard LSTM reducing MAE to 0.097 and CNN-LSTM further lowering it to 0.086. However, RAPS-Net achieves the best overall performance, reaching an MAE of 0.075 and an RMSE of 0.108, representing a 12.8% improvement in RMSE compared with the CNN-LSTM baseline. Moreover, RAPS-Net achieves the highest F1-score of 0.87, outperforming CNN-LSTM by 5 percentage points. This improvement demonstrates the effectiveness of explicitly incorporating IAM permission risks and supply chain features into a unified predictive framework. The high recall value (0.86) further indicates that RAPS-Net is particularly effective at identifying high-risk periods, which is crucial for enabling proactive security control in cloud payment systems.

Table 2. Main Results of Cross-Domain Risk Prediction.

Model	MAE	RMSE	Precision	Recall	F1-score
ARIMA	0.142	0.198	0.71	0.65	0.68
LSTM	0.097	0.134	0.80	0.77	0.78
CNN	0.104	0.146	0.78	0.74	0.76
CNN-LSTM	0.086	0.121	0.84	0.81	0.82
RAPS-Net	0.075	0.108	0.89	0.86	0.87

The ablation results in Table 3 highlight the contribution of each key component in RAPS-Net. Removing permission risk features leads to a notable degradation in performance, increasing RMSE from 0.108 to 0.126 and reducing the F1-score from 0.87 to 0.82. This confirms that IAM misconfigurations and excessive authorization are critical predictors of payment security risk. Similarly, excluding supply chain risk features results in an RMSE of 0.131, demonstrating the importance of operational instability in amplifying payment risks. The absence of the CNN module causes a significant performance drop, with RMSE increasing to 0.143, indicating that local cross-domain feature interactions are essential for accurate risk modeling. Additionally, removing the dynamic control feedback weakens prediction accuracy, suggesting that the closed-loop design contributes to stabilizing risk evolution over time. Overall, the full RAPS-Net configuration consistently delivers the best performance, validating the necessity of integrating permission risk sensing, CNN-LSTM-based prediction, and feedback-driven security control within a unified framework.

Table 3. Ablation Study Results.

Model Variant	MAE	RMSE	Precision
RAPS-Net (Full)	0.075	0.108	0.87

w/o Permission Risk	0.089	0.126	0.82
w/o Supply Chain Risk	0.092	0.131	0.81
w/o CNN Module	0.101	0.143	0.78
w/o Dynamic Control Feedback	0.088	0.124	0.83

The Figure 2 illustrates the training and validation RMSE convergence curves of RAPS-Net and the CNN-LSTM baseline over 60 training epochs. At the early training stage (epochs 1-10), both models exhibit a rapid decrease in RMSE, indicating effective learning of dominant temporal risk patterns. RAPS-Net starts with a training RMSE of approximately 0.28 and a validation RMSE of around 0.30, which decline steadily as training progresses. Notably, RAPS-Net converges faster and more smoothly than CNN-LSTM, reaching a validation RMSE below 0.15 by around epoch 35. In contrast, CNN-LSTM shows a slower convergence trend, with its validation RMSE remaining above 0.15 until approximately epoch 45.

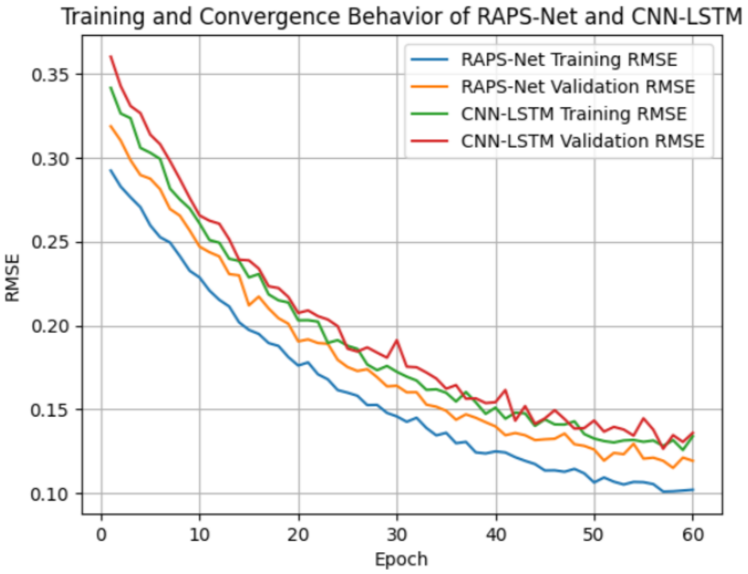

Figure 2. Training and Convergence Behavior of RAPS-Net and CNN-LSTM.

By the end of training, RAPS-Net stabilizes at a validation RMSE of about 0.108, closely matching the main experimental results reported in Table 2, while CNN-LSTM converges to a higher RMSE of approximately 0.121. Mild oscillations are observed in both training and validation curves, reflecting realistic stochastic optimization behavior, but no severe divergence or overfitting occurs. The consistently smaller gap between training and validation curves for RAPS-Net indicates better generalization capability. Overall, the convergence behavior confirms that the proposed RAPS-Net framework achieves faster, more stable training and superior predictive accuracy compared with the CNN-LSTM baseline, validating its effectiveness for cross-domain risk prediction in cloud payment supply chains.

4.5. Discussion

The experimental results demonstrate that RAPS-Net effectively captures the complex interactions between IAM permission risks, supply chain disruptions, and payment system behaviors. Unlike conventional models that focus on isolated risk factors, RAPS-Net provides a holistic and predictive view of cloud payment security. The superior performance across multiple metrics indicates its strong generalization capability and practical value. Moreover, the closed-loop design enables proactive mitigation by translating risk predictions into adaptive access control actions. These findings suggest that risk-aware, prediction-driven security mechanisms represent a promising direction for securing large-scale cloud payment supply chains under dynamic and uncertain operational conditions.

5. Conclusions

This study aims to address the limitations of static access control and isolated risk analysis in cloud payment systems by providing RAPS-Net, a closed-loop framework integrating CNN-LSTM architectures, exploring how cross-domain interactions between IAM permission risks and supply chain disruptions affect payment security. The primary objective of this research is to enable holistic risk perception and proactive, adaptive security control through accurate risk prediction.

Through data analysis, we identified that RAPS-Net significantly outperforms baseline models, reducing RMSE to 0.108 and achieving a 19% improvement over standard LSTM, the integration of CNN and LSTM effectively captures both short-term local risk coupling patterns and long-term evolution trends, and jointly modeling IAM permission risks with supply chain dynamics is essential for accurate risk sensing. These findings suggest that multi-source risk integration and hybrid deep learning enable superior predictive intelligence and robust discriminative power in complex cloud environments.

The results of this study have significantly implications for the field of Cloud Payment Security and Cyber-Physical Systems. Firstly, the discovery of cross-domain risk propagation provides a new perspective on securing financial infrastructures by treating IAM permissions as a first-class security factor. Secondly, the success of the RAPS-Net architecture challenges the existing reliance on single-domain, rule-based security mechanisms. Finally, the prediction-driven dynamic access control mechanism opens new avenues for future research in autonomous security policy management and adaptive cyber-defense.

Despite the important findings, this study has some limitations, such as the use of a dataset partially constructed from simulated and public sources rather than entirely real-world logs and the current focus on threshold-based policy adjustment rather than more complex optimization strategies. Future research could further explore the integration of reinforcement learning for advanced policy optimization and incorporating real-time threat intelligence feeds to improve the robustness and explainability of risk predictions. Specifically, we aim to investigate risk-aware reinforcement learning mechanisms similar to those employed in Uni-FinLLM, which established a macro-micro feedback loop to align predictive outputs with systemic stability goals. Incorporating such adaptive decision-making agents could significantly enhance RAPS-Net's ability to generate more granular, context-aware security policies in response to evolving supply chain disruptions.

In conclusion, this study through the development and experimental validation of a hybrid CNN-LSTM framework, reveals that integrating cross-domain risk signals with predictive modeling enables effective proactive mitigation of security threats, providing new insights for the development next-generation intelligent and resilient cloud payment supply chains.

References

1. B. Liu, Q. Sun, and L. Wei, "Multimodal Forgery Recognition Algorithm and System Design for AI Frauds," In *Proceedings of the 2nd International Symposium on Integrated Circuit Design and Integrated Systems*, September, 2025, pp. 156-160. doi: 10.1145/3772326.3774725
2. S. O. Olabanji, O. O. Olaniyi, C. S. Adigwe, O. J. Okunleye, and T. O. Oladoyinbo, "AI for Identity and Access Management (IAM) in the cloud: Exploring the potential of artificial intelligence to improve user authentication, authorization, and access control within cloud-based systems," *Authorization, and Access Control within Cloud-Based Systems (January 25, 2024)*, 2024. doi: 10.9734/ajrcos/2024/v17i3423
3. L. Golightly, P. Modesti, R. Garcia, and V. Chang, "Securing distributed systems: A survey on access control techniques for cloud, blockchain, IoT and SDN," *Cyber Security and Applications*, vol. 1, p. 100015, 2023. doi: 10.1016/j.csa.2023.100015

4. N. Alharbe, A. Aljohani, M. A. Rakrouki, and M. Khayyat, "An access control model based on system security risk for dynamic sensitive data storage in the cloud," *Applied Sciences*, vol. 13, no. 5, p. 3187, 2023. doi: 10.3390/app13053187
5. Z. Lin, and B. Wang, "Adaptive load balancing algorithms for cloud computing distributed systems," In *IET Conference Proceedings CP952*, October, 2025, pp. 1319-1325. doi: 10.1049/icp.2025.4664
6. M. Saqib, D. Mehta, F. Yashu, and S. Malhotra, "Adaptive security policy management in cloud environments using reinforcement learning," In *2025 International Conference on Metaverse and Current Trends in Computing (ICMCTC)*, April, 2025, pp. 1-10. doi: 10.1109/icmctc62214.2025.11196240
7. V. T. Madireddy, "Graph neural network based adaptive threat detection for cloud identity and access management logs," *arXiv preprint arXiv:2512.10280*, 2025.
8. M. M. Bassiouni, R. K. Chakrabortty, O. K. Hussain, and H. F. Rahman, "Advanced deep learning approaches to predict supply chain risks under COVID-19 restrictions," *Expert Systems with Applications*, vol. 211, p. 118604, 2023. doi: 10.1016/j.eswa.2022.118604
9. W. A. Zogaan, N. Ajabnoor, and A. A. Salamai, "Leveraging deep learning for risk prediction and resilience in supply chains: insights from critical industries," *Journal of Big Data*, vol. 12, no. 1, p. 94, 2025. doi: 10.1186/s40537-025-01143-4
10. W. Gamaleldin, O. Attayyib, M. M. Alnfiai, F. A. Alotaibi, and R. Ming, "A hybrid model based on CNN-LSTM for assessing the risk of increasing claims in insurance companies," *PeerJ Computer Science*, vol. 11, p. e2830, 2025. doi: 10.7717/peerj-cs.2830
11. A. Gupta, and S. Remella, "Privacy-Preserving Smart and Secure Contract Solutions for Digital Supply Chain Payments," *International Journal of AI, BigData, Computational and Management Studies*, vol. 6, no. 4, pp. 232-240, 2025. doi: 10.63282/3050-9416.ijaibdcms-v6i4p127
12. B. Su, G. Gui, S. Xu, and S. Shen, "Study on Real Estate Investment Risk Assessment and Decision Support System Driven by Fintech," In *Proceedings of the 2nd International Symposium on Integrated Circuit Design and Integrated Systems*, September, 2025, pp. 168-174. doi: 10.1145/3772326.3774727

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of GBP and/or the editor(s). GBP and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.