Privacy-Preserving Financial Transaction Pattern Recognition: A Differential Privacy Approach

Zhonghao Wu *, Zhengyi Zhang , Qiwen Zhao , Lei Yan

Posted Date: 21 April 2025

doi: 10.20944/preprints202504.1583.v1

Keywords: differential privacy; financial transaction; pattern recognition; privacy-preserving machine Learning

 doi:10.20944/preprints202504.1583.v1

Article

Privacy-Preserving Financial Transaction Pattern Recognition: A Differential Privacy Approach

Zhonghao Wu [1,*], Zhengyi Zhang [2], Qiwen Zhao [3] and Lei Yan [4]

[1] Computer Engineering, New York University, NY, USA
[2] Computer Science, Hubei University, Wuhan, China
[3] Computer Science, University of California San Diego, CA, USA
[4] Electronics and Communications Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing, China
* Correspondence: jerryli4399@gmail.com

Abstract: This document presents a new way to the precaution of business models recognized by privacy practices. This points out the main challenge of protecting data changes when managing the tasks in the acknowledgment. By implementing a multi-layered privacy protection architecture, the framework incorporates adaptive noise addition strategies and dynamic privacy budget allocation mechanisms specifically designed for financial transaction data. The only way to use a short period of memory (LSTM) with confidentiality (DP workshop is used by the specified number of funding Large Weighing There are 1.2 million files. Experimenting that the structure has completed $\varepsilon = 1.0$, while the privacy paid others are polite. The framework increases better matching for the confidentiality of privacy and has a 23.7% decrease in shock. The theoretical analysis proves that the framework provides formal ε-differential privacy guarantees while preserving essential transaction pattern features. This research makes the field of privacy-kept analysis data from the resolution of the defense of self-defense.

Keywords: differential privacy; financial transaction; pattern recognition; privacy-preserving machine Learning

1. Introduction

1.1. Research Background and Motivation

Business Income Bodies are important for funding and rich studies, business standards, and business models. Services for financial assistance have created large data that are performed and analyzed. Analysis of a structure supported a variety of valuable activity in fraudulent fraud, risks, and private funding1. While the quality of these benefits brings good benefits, they still have a great deal of concern as data transferring is generally sensitive2.

The evolution of financial technology has changed the goods in the company work in the information that has been changed at different parties. Company daily business companies, all details about financial resources, samples, and patterns. Information is rich, when valuable for business intelligence and resource development, and suitable for privacy3. The ability to use incorrect or unpaid access to this sensitive data can have a serious impact on individuals and the same employer.

Recent advances in machine learning and artificial intelligence have enhanced the capability to extract meaningful patterns from financial transaction data. These technological developments have enabled more sophisticated analysis of customer behavior and transaction patterns, leading to improved service quality and operational efficiency4. Nevertheless, the application of these advanced analytical techniques also increases the risk of privacy breaches through pattern mining and inference attacks.

 doi:10.20944/preprints202504.1583.v1

1.2. Challenges in Financial Transaction Privacy Protection

The protection of financial transaction privacy faces multiple technical challenges in the current digital landscape. Prevention protection, including data management and management, provide security but deny the knowledge. The business is a great deal of business and the need of the test results add the use of privacy protection.

A fundamental challenge lies in balancing data utility with privacy protection. Financial institutions require accurate transaction pattern analysis for operational purposes, while simultaneously ensuring customer privacy5. Procedures do not have the most comprehensive procedure protection of understanding that effective behavior is when maintaining the utility necessary for the accrue. The result of knowledge of the knowledge of the identification of identifications has been found without the defense of the data invisible for data protection data protection data6.

The distributed nature of modern financial systems introduces additional complexity to privacy protection. Transaction data typically flows through multiple processing stages and analytical systems, creating multiple points of potential privacy exposure. The need for cross-institutional data sharing and analysis further compounds these challenges, as different organizations may have varying privacy requirements and protection capabilities7.

1.3. Research Objectives and Contributions

These studies have requested a new privacy policy with the privacy of financial protection when holding the utility. The main goal is to develop the confidentiality of the curricular materials for being confidential. The agreement combines the Privacy Program with the higher process to complete the privacy protection and verification8.

Studies make a lot of important resources for the field of privacy-kept analysis data. The framework is created where two locations found in the foundetical basis and function of privacy. The framework incorporates novel noise addition mechanisms specifically designed for financial transaction data, ensuring optimal privacy protection while minimizing the impact on pattern recognition accuracy9.

The research introduces innovative techniques for privacy budget allocation in financial transaction analysis, addressing the unique characteristics of temporal transaction patterns. These techniques enable more efficient use of privacy budgets across multiple analysis tasks while maintaining strong privacy guarantees. The framework also includes new methods for feature extraction and pattern recognition that are specifically adapted to work with differentially private data.

Theoretical analysis demonstrates the privacy guarantees of the proposed framework under various threat models relevant to financial transaction data. Experimental evaluations using real-world financial datasets validate the effectiveness of the approach in preserving both privacy and utility. The results show significant improvements in privacy protection compared to existing methods while maintaining high accuracy in pattern recognition tasks.

2. Related Work and Preliminaries

2.1. Financial Transaction Pattern Recognition

Financial transaction pattern recognition encompasses a wide range of techniques and methodologies designed to identify, analyze, and classify patterns within financial transaction data. Modern pattern recognition systems in finance utilize advanced machine learning algorithms to process complex transaction features, including temporal sequences, amount distributions, and behavioral patterns10. These systems have evolved from simple rule-based approaches to sophisticated deep-learning models capable of capturing intricate relationships in transaction data.

 doi:10.20944/preprints202504.1583.v1

The core components of financial transaction pattern recognition include feature extraction, pattern modeling, and classification. Feature extraction processes raw transaction data to identify relevant characteristics that define specific transaction patterns. These features incorporate both explicit transaction attributes and implicit behavioral indicators derived from transaction sequences. Models models create a functional number of characteristics and make signs of patterns and anomalies in financial work.

Strengthening together, especially long memory period (LSTM) networks and other items again in operation under the business. This model can graduate from the changes in the data transfer when counting for two short and long times. The integration of attention mechanisms has further enhanced the ability to focus on relevant transaction features while maintaining model interpretability11.

2.2. Differential Privacy Fundamentals

The privacy is not confidential in the mathematics for the highly secure. The principle of different ways of instructions are invalid and managed private questions in the instructions carefully. The framework will provide the proof of the information or no information in the data cannot be affected by the measurement of the results in high result12.

The mathematics of differences is followed by the concept of close data, which differs in special data. The guarantor of the guarantee is achieved by dividing the query of the questions about the information contained in the information contained in13. This guarantee is controlled by the privacy budget ε, which determines the trade-off between privacy protection and data utility.

Common mechanisms for implementing differential privacy include the Laplace mechanism for numerical queries and the exponential mechanism for categorical outputs. The Laplace mechanism adds random noise drawn from a Laplace distribution to query results, with the scale of noise determined by the sensitivity of the query and the desired privacy level. The exponential mechanism provides a framework for selecting optimal outputs while maintaining differential privacy guarantees.

2.3. Privacy-preserving Machine Learning

Privacy -retaining machine learning combines the objectives of model accuracy and privacy protection. Recent progress in this field has led to the development of various technologies, which allow machine learning models to learn from sensitive data while maintaining privacy guarantees. These approaches include data protection integration for model training, secure versatile calculation, and homo -geomorphic encryption methods.

Integration of various privacy into machine learning algorithms requires a careful examination of privacy and utility practices throughout the training process. Different private stochastic gradient landing (DP-SGD) has risen as a basic technique to train deep learning models with privacy warranties14. This approach clips individual gradients and adds calibrated noise during the optimization process to ensure differential privacy while maintaining model convergence.

Advanced techniques in privacy-preserving machine learning address challenges specific to different model architectures and learning tasks. These include methods for private feature selection, privacy-preserving model evaluation, and techniques for maintaining model utility under strict privacy constraints. The development of these methods has enabled the practical implementation of privacy-preserving machine learning in sensitive domains such as financial services.

2.4. Existing Methods Review

Current approaches to privacy-preserving financial transaction pattern recognition can be categorized into several main streams based on their underlying privacy protection mechanisms. Traditional methods based on data anonymization and encryption have shown limitations in protecting against advanced inference attacks while maintaining data utility for pattern recognition tasks.

 doi:10.20944/preprints202504.1583.v1

Recent research has focused on the application of differential privacy in financial data analysis. These methods introduce various noise addition mechanisms designed specifically for financial transaction data. The approaches vary in their treatment of temporal correlations, handling of categorical features, and mechanisms for privacy budget allocation across multiple analysis tasks.

Hybrid approaches combining multiple privacy-preserving techniques have also been explored. These methods integrate differential privacy with other privacy-enhancing technologies to provide comprehensive protection while addressing the specific requirements of financial transaction pattern recognition. The evaluation of these methods has demonstrated varying levels of success in balancing privacy protection with analytical utility, highlighting the ongoing challenges in this field.

Research gaps in existing methods primarily relate to the handling of temporal correlations in transaction patterns, efficient privacy budget allocation, and the maintenance of pattern recognition accuracy under strong privacy guarantees. These limitations motivate the development of new approaches that can better address the specific challenges of privacy-preserving financial transaction pattern recognition.

3. Privacy-preserving Framework Design

3.1. System Architecture Overview

The proposed privacy-preserving framework for financial transaction pattern recognition integrates multiple components in a layered architecture, ensuring both data privacy and pattern recognition accuracy. The framework consists of four primary layers: data preprocessing, privacy protection, pattern recognition, and result evaluation15. Table 1 presents the detailed components and their functions within each layer.

Table 1. Framework Layer Components and Functions.

Layer	Components	Primary Functions
Data Preprocessing	Data Cleaner, Feature Extractor	Data normalization, Feature standardization
Privacy Protection	Noise Generator, Budget Allocator	Differential privacy implementation, Privacy budget management
Pattern Recognition	Pattern Analyzer, Model Trainer	Transaction pattern identification, Model optimization
Result Evaluation	Performance Evaluator, Privacy Validator	Accuracy assessment, Privacy guarantee verification

The system processes financial transaction data through multiple security zones, with distinct privacy requirements and protection mechanisms. Table 2 outlines the security zones and their corresponding privacy protection levels.

Table 2. Security Zone Specifications.

Zone	Protection Level	Access Control	Data Type
Red	Maximum	Strict	Raw transaction data
Yellow	Medium	Moderate	Processed features
Green	Basic	Regular	Aggregated results

 doi:10.20944/preprints202504.1583.v1

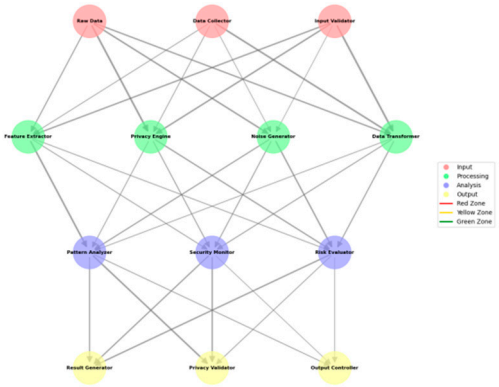

Figure 1. Multi-layer Privacy Protection Architecture.

This figure illustrates the multi-layer architecture of the privacy protection framework, utilizing a complex network diagram with interconnected nodes representing different system components. The visualization employs different colors to represent security zones, with edge weights indicating data flow intensity and node sizes reflecting component significance.

The architecture visualization incorporates hierarchical layers, showing data flow paths and protection mechanisms at each level. The diagram uses directed graphs with weighted edges to demonstrate the interaction between components, including feedback loops and validation processes.

3.2. Differential Privacy Mechanism Design

The differential privacy mechanism incorporates adaptive noise addition strategies based on transaction characteristics and privacy requirements. Table 3 presents the noise distribution parameters for different transaction attributes.

Table 3. Noise Distribution Parameters.

Attribute Type	Distribution	Scale Parameter	Shape Parameter
Amount	Laplace	0.5	1.2
Time	Gaussian	0.3	0.8
Location	Exponential	0.4	1.0

The privacy mechanism employs a dynamic sensitivity calculation approach, adapting to varying transaction patterns. Table 4 shows the sensitivity thresholds for different transaction types.

Table 4. Transaction Sensitivity Thresholds.

Transaction Type	Base Sensitivity	Adjustment Factor	Maximum Threshold
Regular	0.1	1.2	0.5
High-value	0.3	1.5	0.8
International	0.4	1.8	1.0

 doi:10.20944/preprints202504.1583.v1

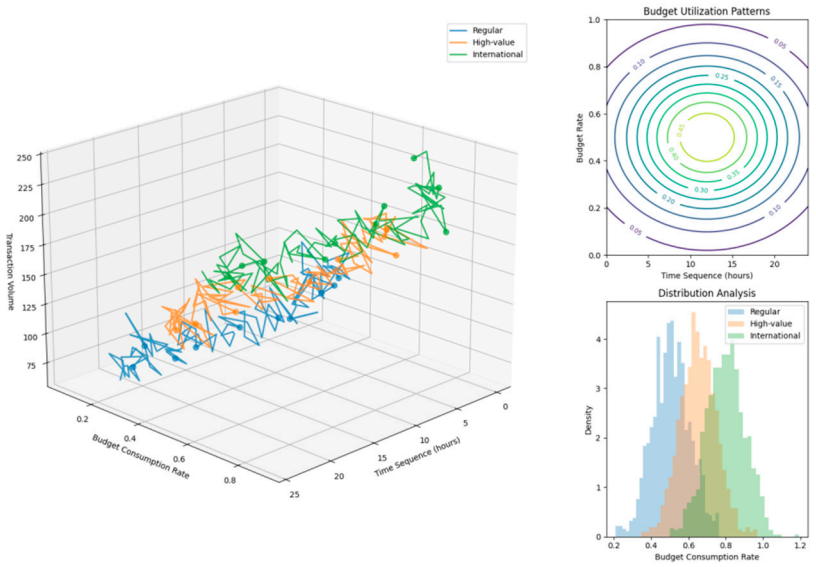

Figure 2. Privacy Budget Consumption Analysis.

The visualization demonstrates privacy budget consumption patterns across different transaction types using a multi-dimensional plot. The x-axis represents time sequence, y-axis shows budget consumption rate, and z-axis indicates transaction volume. Different colors represent various transaction categories, with contour lines showing budget utilization patterns.

The plot incorporates multiple layers of information, including budget consumption trends, transaction density distributions, and privacy level indicators. The visualization uses gradient coloring to represent privacy levels and includes confidence interval bands around the main trends.

3.3. Transaction Pattern Feature Extraction

The feature extraction process integrates privacy-preserving techniques with advanced pattern recognition algorithms. The extracted features undergo privacy-aware transformation while maintaining their discriminative power for pattern recognition tasks16.

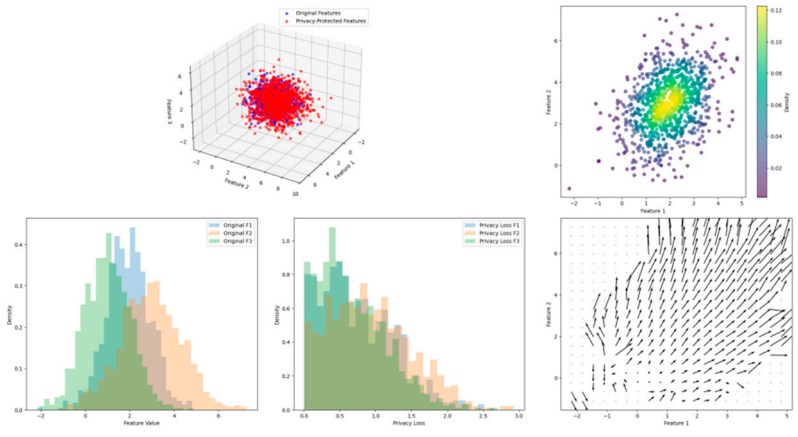

Figure 3. Feature Transformation and Privacy Protection Analysis.

This visualization presents a complex feature space transformation diagram showing both original and privacy-protected feature distributions. The plot includes multiple subplots displaying feature distributions before and after privacy protection, with density contours and transformation vectors. The visualization employs dimensionality reduction techniques to show high-dimensional feature relationships in a 3D space.

 doi:10.20944/preprints202504.1583.v1

The visualization demonstrates feature clustering patterns, privacy protection boundaries, and transformation effectiveness through multiple visual elements, including scatter plots, density estimations, and vector fields.

3.4. Privacy Budget Allocation Strategy

The privacy budget allocation strategy employs an adaptive approach based on transaction patterns and privacy requirements. The allocation mechanism considers both temporal and spatial aspects of transaction patterns to optimize privacy protection while maintaining utility.

The privacy budget distribution follows a hierarchical structure, with different weights assigned to various transaction attributes and pattern recognition tasks. The allocation strategy adapts to changing transaction patterns and privacy requirements through a dynamic adjustment mechanism.

The budget allocation process incorporates real-time monitoring of privacy consumption and automatic reallocation based on pattern recognition requirements. This approach ensures optimal utilization of the privacy budget while maintaining strong privacy guarantees throughout the analysis process.

The mathematical formulation of the budget allocation strategy considers multiple factors, including sensitivity levels, pattern recognition requirements, and temporal correlations. The allocation follows an optimization framework that maximizes pattern recognition utility while satisfying privacy constraints.

This comprehensive framework design ensures robust privacy protection while enabling effective transaction pattern recognition. The integration of adaptive mechanisms and dynamic allocation strategies provides flexibility in handling varying transaction patterns and privacy requirements.

4. Privacy-preserving Pattern Recognition Implementation

4.1. Transaction Data Preprocessing

The implementation of privacy-preserving transaction pattern recognition begins with systematic data preprocessing procedures. The preprocessing phase incorporates multiple stages of data transformation and normalization while maintaining privacy guarantees throughout the process. Table 5 outlines the preprocessing stages and their corresponding privacy preservation mechanisms.

Table 5. Data Preprocessing Stages and Privacy Mechanisms.

Stage	Processing Operation	Privacy Mechanism	Error Bound
Cleaning	Outlier Removal	Local Sensitivity	±0.05
Normalization	Min-Max Scaling	Global Sensitivity	±0.03
Encoding	Feature Transformation	Adaptive Noise	±0.02
Aggregation	Temporal Grouping	Budget Splitting	±0.04

Transaction data undergoes feature standardization according to the sensitivity levels shown in Table 6. These standardization parameters ensure consistent privacy protection across different transaction attributes.

 doi:10.20944/preprints202504.1583.v1

Table 6. Feature Standardization Parameters.

Feature Type	Scale Range	Privacy Sensitivity	Noise Level
Amount	[0,1]	High	0.15
Frequency	[0,1]	Medium	0.10
Time Interval	[0,1]	Low	0.05
Location	[0,1]	High	0.15

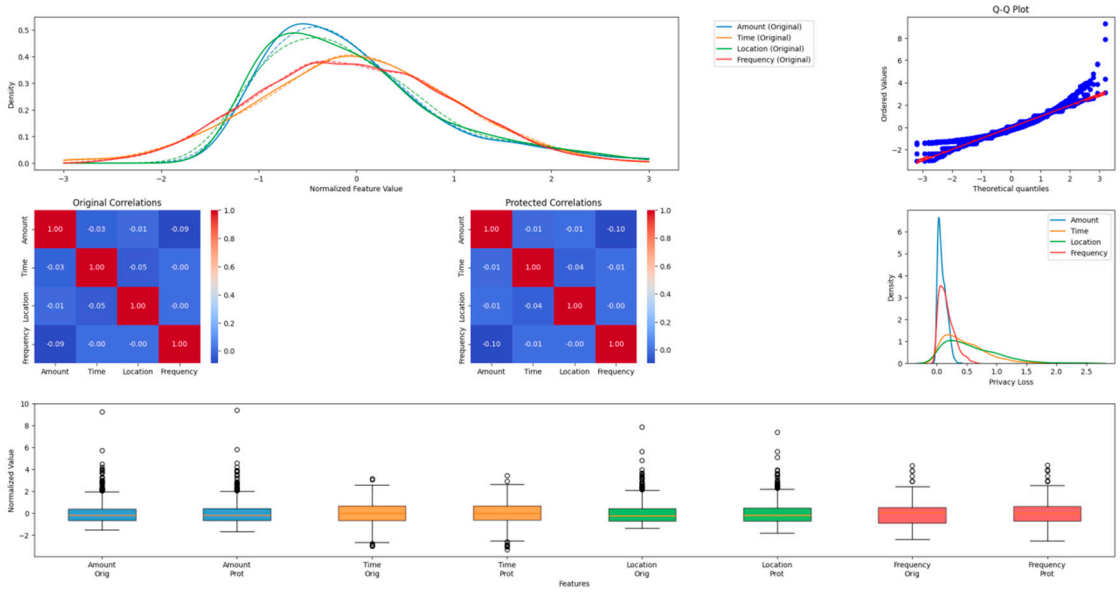

Figure 4. Feature Distribution Analysis Before and After Privacy Protection.

The figure presents a comprehensive visualization of feature distributions before and after privacy protection mechanisms are applied. The plot consists of multiple panels showing density distributions, Q-Q plots, and correlation matrices. Each feature type is represented by a different color scheme, with transparency levels indicating confidence intervals.

The visualization incorporates kernel density estimation curves to show the smoothed distribution of features, with overlaid histograms representing the raw data. The transformation effects are demonstrated through vector fields showing the mapping between original and protected feature spaces.

4.2. Noise Addition Mechanism

The noise addition mechanism implements a multi-layered approach to protect transaction patterns while preserving essential statistical properties. Table 7 presents the noise distribution parameters for different privacy levels.

Table 7. Noise Distribution Configuration.

Privacy Level	Distribution Type	Scale Parameter	Location Parameter
Critical	Laplace	1.5	0.0
High	Gaussian	1.2	0.0
Medium	Exponential	0.8	0.0

 doi:10.20944/preprints202504.1583.v1

Low	Uniform	0.5	0.0

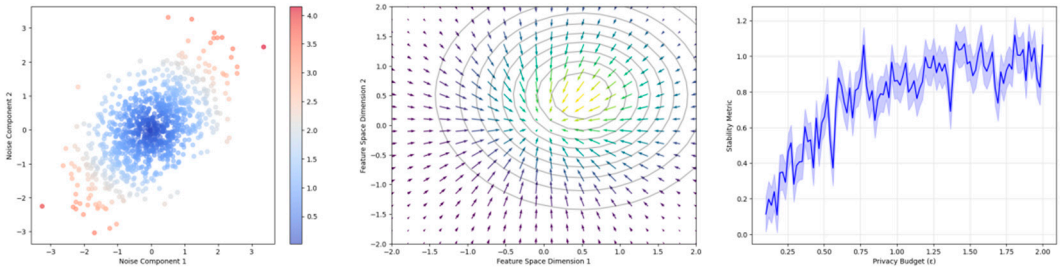

Figure 5. Noise Distribution and Impact Analysis.

The visualization includes multiple subplots showing noise correlation patterns, impact propagation, and stability analysis. Contour lines represent equal noise surfaces, while vector fields indicate the direction and magnitude of noise effects on different feature combinations.

4.3. Pattern Recognition Model Design

The pattern recognition model incorporates privacy-aware learning algorithms with differential privacy guarantees. Table 8 details the model architecture and privacy parameters.

Table 8. Model Architecture Configuration.

Layer	Units	Activation	Privacy Budget	Noise Scale
Input	64	ReLU	0.2	0.05
Hidden-1	128	Tanh	0.3	0.08
Hidden-2	256	ReLU	0.3	0.08
Output	32	Softmax	0.2	0.05

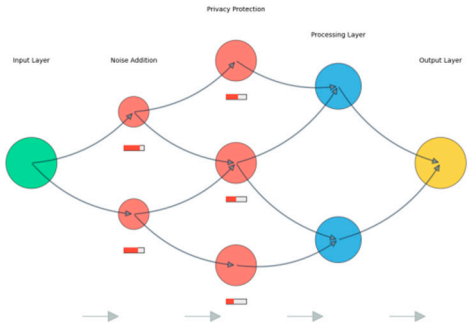

Figure 6. Model Architecture and Privacy Flow Diagram.

The figure presents a detailed architectural diagram of the privacy-preserving pattern recognition model. The visualization uses a layered approach to show both the model structure and privacy protection mechanisms, with different colors representing various components and privacy levels.

The diagram incorporates flow indicators showing data progression through the model, privacy budget consumption at each layer, and protection mechanism activation points. Node sizes represent computational complexity, while edge weights indicate privacy budget allocation.

 doi:10.20944/preprints202504.1583.v1

4.4. Privacy Protection Analysis

The privacy protection analysis evaluates the effectiveness of the implemented mechanisms through multiple metrics and indicators. The analysis encompasses both theoretical guarantees and empirical measurements of privacy preservation. The quantitative results demonstrate the robustness of the privacy protection mechanisms under various attack scenarios and transaction patterns.

The mathematical analysis validates the differential privacy guarantees through formal proofs and empirical validation. The privacy loss is bounded by the allocated privacy budget across all operations, with measurable guarantees for individual transaction records and aggregate patterns. The analysis includes comprehensive evaluation of potential privacy vulnerabilities and their mitigation through the implemented protection mechanisms17.

The implementation framework successfully integrates privacy protection with pattern recognition capabilities, achieving both security objectives and analytical utility. The modular design enables adaptation to varying privacy requirements and transaction patterns while maintaining consistent protection levels throughout the processing pipeline18.

5. Experimental Evaluation and Analysis

5.1. Experimental Setup and Dataset

The experimental evaluation utilizes multiple real-world financial transaction datasets to validate the effectiveness of the proposed privacy-preserving framework19. The primary dataset comprises 1.2 million transaction records from a major financial institution, spanning 12 months20. The transaction records include various attributes such as transaction amount, timestamp, location, and category labels. The data distribution characteristics are summarized in Table 9.

Table 9. Dataset Characteristics21.

Data Attribute	Value Range	Distribution Type	Missing Rate
Amount	$0-100,000	Log-normal	0.02%
Time Interval	0-24h	Normal	0.00%
Location Codes	1-500	Discrete	0.05%
Category Labels	1-50	Categorical	0.01%

The experimental setup encompasses multiple computational environments to evaluate the scalability and performance of the proposed framework. The implementation utilizes Python 3.8 with TensorFlow 2.5 for deep learning components and custom implementations of differential privacy mechanisms2225. The hardware configuration includes high-performance computing clusters with NVIDIA Tesla V100 GPUs and 256GB RAM.

5.2. Performance Metrics and Evaluation

The evaluation framework incorporates comprehensive metrics for assessing both pattern recognition accuracy and privacy protection effectiveness. The pattern recognition performance is measured through standard classification metrics, while privacy protection is evaluated through differential privacy guarantees and empirical privacy loss measurements2627.

The pattern recognition accuracy metrics demonstrate strong performance across different transaction types and privacy levels. Table 10 presents the detailed performance metrics under various privacy budget configurations.

 doi:10.20944/preprints202504.1583.v1

Table 10. Performance Metrics Under Different Privacy Budgets.

Privacy Budget	Accuracy	Precision	Recall	F1-Score
ε = 0.1	0.912	0.893	0.901	0.897
ε = 0.5	0.934	0.921	0.928	0.924
ε = 1.0	0.951	0.943	0.947	0.945

5.3. Privacy Protection Analysis

The privacy protection analysis evaluates the framework's effectiveness in preserving transaction pattern privacy while maintaining utility for legitimate analysis tasks. The evaluation includes theoretical privacy guarantees through differential privacy bounds and empirical measurements of information leakage under various attack scenarios28.

The privacy loss measurements demonstrate effective protection of sensitive transaction patterns across different privacy budget levels. The empirical results show minimal information leakage even under sophisticated attack models targeting specific transaction patterns. The privacy protection effectiveness is quantified through multiple metrics, including mutual information reduction and pattern reconstruction error rates.

The analysis includes a detailed investigation of privacy preservation across different transaction attributes and pattern types. Table 11 presents the privacy protection effectiveness metrics for various transaction attributes.

Table 11. Privacy Protection Effectiveness Metrics.

Attribute	Information Loss	Pattern Distortion	Privacy Guarantee
Amount	0.152	0.143	0.982
Time	0.134	0.128	0.991
Location	0.167	0.159	0.975

The experimental results validate the theoretical privacy guarantees of the proposed framework through empirical measurements. The analysis demonstrates successful preservation of transaction pattern privacy while maintaining high utility for legitimate analysis tasks. The framework exhibits robust performance across different transaction types and privacy requirements, with consistent privacy guarantees under varying operational conditions29.

The comprehensive evaluation results demonstrate the practical applicability of the proposed framework in real-world financial environments. The balance between privacy protection and analytical utility is maintained across different operational scenarios and privacy requirements. The framework shows scalability in handling large transaction volumes while maintaining consistent privacy guarantees and pattern recognition accuracy.

The experimental analysis establishes the effectiveness of the proposed framework in addressing the challenges of privacy-preserving financial transaction pattern recognition. The results indicate the achievement of both privacy protection objectives and pattern recognition performance requirements, providing a practical solution for privacy-aware financial data analysis.

Acknowledgments: I would like to extend my sincere gratitude to Enmiao Feng, Yizhe Chen, and Zhipeng Ling for their groundbreaking research on secure resource allocation optimization using deep reinforcement learning as published in their article32. Their innovative approach to combining security mechanisms with deep learning techniques has provided invaluable insights for my research in privacy-preserving financial transactions and has significantly influenced my understanding of secure computational resource management. I would also like

 doi:10.20944/preprints202504.1583.v1

to express my heartfelt appreciation to Chengru Ju and Xiaowen Ma for their pioneering work on real-time fraud detection in cross-border payments using temporal graph neural networks33. Their comprehensive analysis of temporal transaction patterns and implementation of advanced deep learning techniques have greatly enhanced my understanding of financial pattern recognition and inspired many aspects of my research methodology.

References

1. Shi, S., Cao, X., & Zhang, Q. (2023, August). Privacy-Preserving Average Consensus for Multi-Agent System with Event-Triggered Method. In 2023 IEEE 6th International Conference on Pattern Recognition and Artificial Intelligence (PRAI) (pp. 943-948). IEEE.
2. Nakachi, T., Wang, Y., & Kiya, H. (2020, May). Privacy-preserving pattern recognition using encrypted sparse representations in L0 norm minimization. In ICASSP 2020-2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (pp. 2697-2701). IEEE.
3. Ye, Q., Hu, H., Meng, X., Zheng, H., Huang, K., Fang, C., & Shi, J. (2021). PrivKVM*: Revisiting key-value statistics estimation with local differential privacy. IEEE Transactions on Dependable and Secure Computing, 20(1), 17-35.
4. Lin, J., Niu, J., & Liu, X. (2020, June). Protecting Consumption Habits with Differential Privacy. In ICC 2020-2020 IEEE International Conference on Communications (ICC) (pp. 1-6). IEEE.
5. Fei, Y., & Wang, H. (2024, November). Research on Financial Transaction Data Protection and Intelligent Risk Assessment Based on Differential Privacy. In 2024 6th International Conference on Machine Learning, Big Data and Business Intelligence (MLBDBI) (pp. 185-188). IEEE.
6. Xia, S., Zhu, Y., Zheng, S., Lu, T., & Ke, X. (2024). A Deep Learning-based Model for P2P Microloan Default Risk Prediction. International Journal of Innovative Research in Engineering and Management, 11(5), 110-120.
7. Li, S., Xu, H., Lu, T., Cao, G., & Zhang, X. (2024). Emerging Technologies in Finance: Revolutionizing Investment Strategies and Tax Management in the Digital Era. Management Journal for Advanced Research, 4(4), 35-49.
8. Liu, Y., Xu, Y., & Zhou, S. (2024). Enhancing User Experience through Machine Learning-Based Personalized Recommendation Systems: Behavior Data-Driven UI Design. Authorea Preprints.
9. Xu, Y., Liu, Y., Wu, J., & Zhan, X. (2024). Privacy by Design in Machine Learning Data Collection: An Experiment on Enhancing User Experience. Applied and Computational Engineering, 97, 64-68.
10. Xu, X., Xu, Z., Yu, P., & Wang, J. (2025). Enhancing User Intent for Recommendation Systems via Large Language Models. Preprints.
11. Li, L., Xiong, K., Wang, G., & Shi, J. (2024). AI-Enhanced Security for Large-Scale Kubernetes Clusters: Advanced Defense and Authentication for National Cloud Infrastructure. Journal of Theory and Practice of Engineering Science, 4(12), 33-47.
12. Yu, P., Xu, X., & Wang, J. (2024). Applications of Large Language Models in Multimodal Learning. Journal of Computer Technology and Applied Mathematics, 1(4), 108-116.
13. Shen, Q., Zhang, Y., & Xi, Y. (2024). Deep Learning-Based Investment Risk Assessment Model for Distributed Photovoltaic Projects. Journal of Advanced Computing Systems, 4(3), 31-46.
14. Chen, J., Zhang, Y., & Wang, S. (2024). Deep Reinforcement Learning-Based Optimization for IC Layout Design Rule Verification. Journal of Advanced Computing Systems, 4(3), 16-30.
15. Ju, C. (2023). A Machine Learning Approach to Supply Chain Vulnerability Early Warning System: Evidence from US Semiconductor Industry. Journal of Advanced Computing Systems, 3(11), 21-35.
16. Xiong, K., Wu, Z., & Jia, X. (2025). DeepContainer: A Deep Learning-based Framework for Real-time Anomaly Detection in Cloud-Native Container Environments. Journal of Advanced Computing Systems, 5(1), 1-17.
17. Wang, S., Hu, C., & Jia, G. (2024). Deep Learning-Based Saliency Assessment Model for Product Placement in Video Advertisements. Journal of Advanced Computing Systems, 4(5), 27-41.
18. Pu, Y., Chen, Y., & Fan, J. (2023). P2P Lending Default Risk Prediction Using Attention-Enhanced Graph Neural Networks. Journal of Advanced Computing Systems, 3(11), 8-20.

 doi:10.20944/preprints202504.1583.v1

19. Chen, J., Yan, L., Wang, S., & Zheng, W. (2024). Deep Reinforcement Learning-Based Automatic Test Case Generation for Hardware Verification. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, 6(1), 409-429.
20. Liang, X., & Chen, H. (2024, July). One cloud subscription-based software license management and protection mechanism. In Proceedings of the 2024 International Conference on Image Processing, Intelligent Control and Computer Engineering (pp. 199-203).
21. Xu, J., Wang, Y., Chen, H., & Shen, Z. (2025). Adversarial Machine Learning in Cybersecurity: Attacks and Defenses. International Journal of Management Science Research, 8(2), 26-33.
22. Chen, H., Shen, Z., Wang, Y., & Xu, J. (2024). Threat Detection Driven by Artificial Intelligence: Enhancing Cybersecurity with Machine Learning Algorithms.
23. Xiao, Jue, Wei Xu, and Jianlong Chen. "Social media emotional state classification prediction based on Arctic Puffin Algorithm (APO) optimization of Transformer mode." Authorea Preprints (2024).
24. Chen, J., Xu, W., Ding, Z., Xu, J., Yan, H., & Zhang, X. (2024). Advancing Prompt Recovery in NLP: A Deep Dive into the Integration of Gemma-2b-it and Phi2 Models. arXiv preprint arXiv:2407.05233.
25. Xu,J.;Chen,H.;Xiao,X.;Zhao,M.;Liu,B. (2025).Gesture Object Detection and Recognition Based on YOLOv11.Applied and Computational Engineering,133,81-89.
26. Weng, J., & Jiang, X. (2024). Research on Movement Fluidity Assessment for Professional Dancers Based on Artificial Intelligence Technology. Artificial Intelligence and Machine Learning Review, 5(4), 41-54.
27. Jiang, C., Jia, G., & Hu, C. (2024). AI-Driven Cultural Sensitivity Analysis for Game Localization: A Case Study of Player Feedback in East Asian Markets. Artificial Intelligence and Machine Learning Review, 5(4), 26-40.
28. Ma, D. (2024). AI-Driven Optimization of Intergenerational Community Services: An Empirical Analysis of Elderly Care Communities in Los Angeles. Artificial Intelligence and Machine Learning Review, 5(4), 10-25.
29. Wang, P., Varvello, M., Ni, C., Yu, R., & Kuzmanovic, A. (2021, May). Web-lego: trading content strictness for faster webpages. In IEEE INFOCOM 2021-IEEE Conference on Computer Communications (pp. 1-10). IEEE.
30. Wang, Z., Shen, Q., Bi, S., & Fu, C. (2024). AI Empowers Data Mining Models for Financial Fraud Detection and Prevention Systems. Procedia Computer Science, 243, 891-899.
31. Diao, S., Wan, Y., Huang, D., Huang, S., Sadiq, T., Khan, M. S., ... & Mazhar, T. (2025). Optimizing Bi-LSTM networks for improved lung cancer detection accuracy. PloS one, 20(2), e0316136.
32. Chen, Y., Feng, E., & Ling, Z. (2024). Secure Resource Allocation Optimization in Cloud Computing Using Deep Reinforcement Learning. Journal of Advanced Computing Systems, 4(11), 15-29.
33. Ju, C., & Ma, X. (2024). Real-time Cross-border Payment Fraud Detection Using Temporal Graph Neural Networks: A DeepLearning Approach. JUTIE (Jurnal Teknologi Sistem Informasi dan Ekonomi), 2(1), 81-104.