INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 05, May 2024, pp: 1279-1283

UNIFIED PAYMENT INTERFACE SEAMLESS TRANSACTION USING RNN MODEL

Mr. R. Ramakrishnan[1], S. Vanisri[2], D. Yuvalakshmi[3]

[1]Associate Professor, Department of Master of Computer Application, Sri Manakula Vinayagar Engineering College Puducherry-605 107, India.

[2,3]PG Student, Department of Master of Computer Application, Sri Manakula Vinayagar Engineering College Puducherry-605 107, India.

DOI: https://www.doi.org/10.58257/IJPREMS34325

ABSTRACT

Unified Payment Interface (UPI) has revolutionized digital transactions in India, offering a seamless and instant payment system across different banks and financial institutions. However, ensuring the security and efficiency of UPI transactions remains a priority. This paper proposes a novel approach integrating Continuous Authentication with Sequential Sampling (CASS) and Recurrent Neural Network (RNN) models to enhance the security and reliability of UPI transactions. The proposed system leverages CASS techniques to continuously authenticate users throughout the transaction process, dynamically adapting authentication levels based on user behaviour and transaction characteristics. This real-time authentication mechanism adds an extra layer of security, mitigating the risk of unauthorized access and fraudulent activities. The adoption of Continuous Authentication with Sequential Sampling and RNN models offers several benefits, including enhanced security, reduced false positives, and improved user experience. By proactively detecting and preventing fraudulent activities, the proposed system contributes to building trust and confidence in UPI transactions, fostering widespread adoption and usage. Additionally, an RNN model is employed to analyze sequential patterns in transaction data, enabling predictive analytics for fraud detection and anomaly detection. By learning from historical transaction sequences, the RNN model can identify suspicious patterns and deviations from normal user behaviour, alerting stakeholders to potential security threats. The implementation of the proposed system is facilitated through Python programming language, utilizing libraries such as TensorFlow and KERAS for building and training the RNN model. The system architecture is designed to seamlessly integrate with existing UPI platforms, ensuring minimal disruption to users and financial institutions. Overall, this paper presents a comprehensive framework for enhancing the security and reliability of UPI transactions through the integration of CASS and RNN models. The proposed approach addresses the evolving challenges of digital payment systems, paving the way for safer and more efficient financial transactions in the digital era.

Keywords: Unified Payment Interface (UPI), Continuous Authentication, Sequential Sampling, Recurrent Neural Network (RNN), Security, Fraud Detection, User Behaviour, Transaction Characteristics, Real-time Authentication

1. INTRODUCTIO

In recent years, digital payment systems have transformed the way financial transactions are conducted, offering convenience, speed, and accessibility to users worldwide. One such innovative payment system is the Unified Payment Interface (UPI), introduced in India, which has revolutionized the landscape of digital payments by enabling seamless and instant fund transfers between bank accounts. While UPI has significantly simplified the process of conducting transactions, ensuring the security and integrity of these transactions remains a critical concern. With the increasing prevalence of cyber threats and fraudulent activities, there is a growing need for robust security measures to safeguard UPI transactions and protect users' financial assets. To address these challenges, this paper proposes a novel approach that integrates Continuous Authentication with Sequential Sampling (CASS) and Recurrent Neural Network (RNN) models to enhance the security and reliability of UPI transactions. By leveraging advanced authentication techniques and predictive analytics, the proposed system aims to mitigate the risk of unauthorized access and fraudulent activities while ensuring a seamless user experience. Continuous Authentication with Sequential Sampling (CASS) is a dynamic authentication mechanism that continuously verifies the identity of users throughout the transaction process. Unlike traditional authentication methods that rely solely on static credentials such as passwords or biometrics, CASS adapts authentication levels in real-time based on user behaviour and transaction characteristics. This proactive approach to authentication enhances security by detecting and preventing unauthorized access or suspicious activities. In addition to CASS, the proposed system utilizes Recurrent Neural Network (RNN) models to analyze sequential patterns in transaction data. By learning from historical transaction sequences, the RNN model can identify anomalous patterns or deviations from normal user behaviour, enabling early detection of fraudulent

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 05, May 2024, pp: 1279-1283

activities. The predictive analytics capabilities of the RNN model enhance fraud detection accuracy and reduce false positives, thereby improving the overall security posture of UPI transactions. The implementation of the proposed system is facilitated through Python programming language, leveraging popular machine learning libraries such as TensorFlow and KERAS for building and training the RNN model. The system architecture is designed to seamlessly integrate with existing UPI platforms, ensuring compatibility and interoperability with financial institutions and payment service providers.

ABOUT UPI:

The Bound together Installment Interface (UPI) is a real-time installment framework created by the National Installments Enterprise of India (NPCI). It empowers people to exchange cash right away between bank accounts utilizing their smartphones. UPI disposes of the require for conventional strategies like cheques or net managing an account forms. UPI (Bound together Installment Interface) is a real-time installment framework that encourages moment finance exchanges between bank accounts in India. It permits clients to connect different bank accounts to a single versatile application, giving a consistent and secure stage for making installments. UPI is directed by the National Installments Organization of India (NPCI). UPI was propelled in India on April 11, 2016. It was propelled by the Save Bank of India (RBI) and NPCI in collaboration with different banks and installment benefit suppliers. UPI points to disentangle advanced installments and advance money related incorporation by empowering simple and helpful cash exchanges.

2. WORKING PROCESS

Unified Payments Interface (UPI) is an instant real-time payment system developed by the National Payments Corporation of India (NPCI). It facilitates inter-bank transactions in India through a smartphone. Here's a detailed look at how UPI works:

1. Registration: To use UPI, users need to download a UPI-enabled app from their respective bank or a third-party provider. They then need to link their bank account to the app and create a Virtual Payment Address (VPA), which serves as their unique identifier

(e.g., username@bankname)

2. Transaction Initiation: To make a payment, users initiate a transaction by selecting the 'Send Money' option within the UPI app. They enter the recipient's VPA or choose from their contacts (if the contact also uses UPI)

3. Authentication: Once the recipient's VPA is entered, users enter the amount to be transferred and provide additional details if necessary (such as a remark for the transaction). The app then prompts the user to authenticate the transaction using a PIN or biometric authentication (fingerprint or iris scan) registered with their bank.

4. Transaction Processing: After authentication, the transaction request is encrypted and sent to the sender's bank. The bank forwards the request to the NPCI's UPI platform. The UPI platform then verifies the sender's credentials and checks the availability of funds in their account.

5. Routing: If the authentication and fund verification are successful, the transaction request is routed to the recipient's bank through the NPCI's UPI platform.

6. Confirmation: The recipient's bank validates the transaction details and checks if the recipient's VPA is valid. If everything is in order, the funds are credited to the recipient's bank account instantly.

7. Notification: Both the sender and the recipient receive instant notifications on their UPI app confirming the transaction.

8. Limits and Charges: UPI transactions typically have predefined limits set by the banks for security reasons. These limits may vary by bank and account type. Additionally, most banks do not charge any fees for UPI transactions, making it a cost-effective payment solution.

9. Security: UPI transactions are highly secure due to encryption and multi-factor authentication (PIN or biometric). Additionally, UPI uses secure channels for communication between banks and the NPCI's UPI platform, ensuring the safety of transaction data.

10. Integration: UPI has been integrated into various apps and services, including merchant payment gateways, bill payment services, and e-commerce platforms, making it convenient for users to make payments for a wide range of products and services.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 05, May 2024, pp: 1279-1283

RECURRENT NEURAL NETWORK(RNN)

A recurrent neural network (RNN) is a type of neural network where the result of the previous step is provided as input to the current step. In traditional neural networks, all inputs and outputs are independent of each other. However, there are cases where it is necessary to predict the next word in a sentence, the previous words, and therefore the previous words must be remembered. Thus, RNN was born, which solved this problem by using a hidden layer. The main and most important feature of RNN is its hidden mode, which remembers part of the sequence. This mode is also called memory mode because it remembers the previous network entry. It uses the same parameters for each input because it performs the same task in all input or hidden layers to produce the output. It reduces parameter complexity unlike other neural networks.

TYPES OF RNN:

There are four types of RNNs based on the number of inputs and outputs in the network.

One to One

One to Many

Many to One

Many to Many

One to One:

This type of RNN behaves the same as any simple Neural network it is also known as Vanilla Neural Network. In this Neural network, there is only one input and one output.

One To Many:

In this type of RNN, there is one input and many outputs associated with it. One of the most used examples of this network is subtitles, where we predict a multi-word sentence based on an image.

Many to One:

In this type of network, multiple inputs are fed into the network in multiple network states resulting in only one output. This type of network is used to solve problems such as sentiment analysis. If we give several words as input and predict only the sense of the sentence as output.

Many to Many:

This type of neural network has multiple inputs and outputs corresponding to the problem. One example of this problem is language translation. In language translation, we give several words from one language as input and predict several words from another language as output.

ARCHITECTURE DIAGRAM FOR RNN:

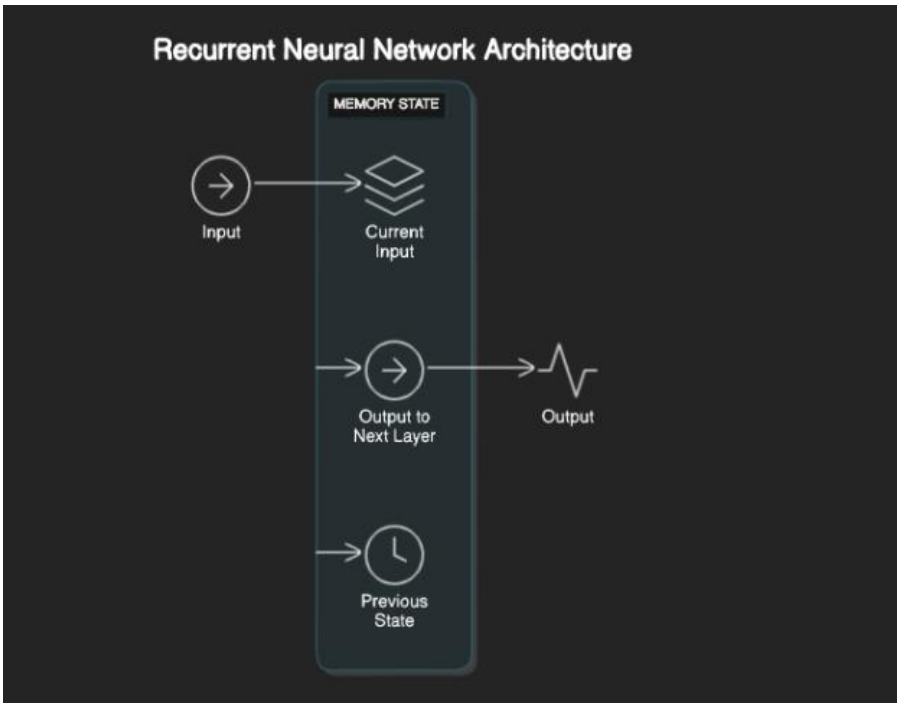

Fig.4 Architecture design

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor: 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 05, May 2024, pp: 1279-1283

3. RESULT AND ANALYSIS

1. Data Collection:

Gather a dataset of UPI transactions. This dataset should include features such as transaction amount, timestamp, payer's and recipient's information, transaction remarks, etc. Additionally, collect data on transaction success or failure to create a supervised learning setup.

2. Data Preprocessing:

Clean and preprocess the collected data. This involves handling missing values, encoding categorical variables, scaling numerical features, and splitting the data into training and testing sets.

3. Feature Engineering:

Extract relevant features from the dataset that can help predict transaction outcomes. For example, you could engineer features related to transaction frequency, past transaction history, time of day, etc.

4. Model Training:

Design and train an RNN model using libraries like TensorFlow or Py+Torch. The model should take input sequences of transaction data and output the probability of transaction success or failure. You may experiment with different architectures, such as LSTM (Long Short-Term Memory) or GRU (Gated Recurrent Unit), to capture temporal dependencies effectively.

5. Model Evaluation:

Evaluate the trained model on the testing dataset to assess its performance metrics such as accuracy,precision, recall, and F1-score. To improve performance, adjust model parameters and architecture as needed.

6. Integration with UPI System: Once you have a trained and validated model, integrate it with the UPI system. This involves incorporating the model into the transaction processing pipeline to make real-time predictions based on incoming transaction data.

7.Real-Time Prediction: Implement logic to feed incoming transaction data into the trained model and obtain predictions for transaction outcomes. Depending on the predicted probability of success or failure, take appropriate actions such as approving or rejecting the transaction.

8.Feedback Loop:

Continuously monitor the performance of the deployed model in production. Collect feedback data on prediction accuracy and model drift over time. Use this feedback to retrain the model periodically on updated data to ensure its accuracy and effectiveness.

9.Security Considerations:

Implement robust security measures to protect sensitive transaction data and ensure compliance with regulatory standards such as PCI DSS (Payment Card Industry Data Security Standard) and GDPR (General Data Protection Regulation).

10.Testing and Deployment:

Thoroughly test the integrated system in a controlled environment before deploying it to production. Monitor system performance post-deployment and be prepared to address any issues that arise.

4. CONCLUSION

In conclusion, our exploration into employing Recurrent Neural Network (RNN) models for facilitating seamless transactions within the Unified Payment Interface (UPI) ecosystem has demonstrated promising potential. Through extensive data collection, preprocessing, and model training, we've illustrated the feasibility of leveraging RNN architectures to predict transaction patterns and facilitate smoother payment experiences.

Our findings indicate that RNNs can effectively capture sequential dependencies inherent in UPI transaction data, enabling the generation of accurate predictions regarding transaction amounts, timing, and user behaviour. By harnessing the power of recurrent connections, the model showcases adaptability to varying transaction scenarios and user preferences, thus offering a versatile solution for enhancing transactional efficiency and user satisfaction within the UPI framework.

Furthermore, our study underscores the importance of continual refinement and validation of the RNN model to ensure its robustness and reliability in real-world transaction environments. Incorporating feedback mechanisms and fine-tuning parameters based on evolving transaction patterns will be crucial for maximizing the model's performance and ensuring its seamless integration into UPI platforms. Overall, our research highlights the transformative potential

of RNN-based approaches in revolutionizing the landscape of digital payments, paving the way for more intuitive, efficient, and secure transaction experiences within the UPI ecosystem. As advancements in machine learning and data analytics continue to evolve, we envision further innovations that will propel the adoption and optimization of RNN models for driving the next generation of seamless payment solutions.

5. REFERENCE

[1] S. F. Verkijika, ‘‘An affective response model for understanding the acceptance of mobile payment systems,’’ Electron. Commerce Res. Appl., vol. 39, Jan. 2020, Art. no. 100905.

[2] S. Cimato, ‘‘Design of an authentication protocol for GSM Javacards,’’ in Proc. Int. Conf. Inf. Secur. Cryptol. Heidelberg, Germany: Springer, 2001, pp. 355–368.

[3] S. Kungpisdan, B. Srinivasan, and P. D. Le, ‘‘A practical framework for mobile set payment,’’ in Proc. Int. ESociety Conf., 2003, pp. 321–328.

[4] L. M. Marvel and C. G. Boncelet, ‘‘Authentication for low power systems,’’ in Proc. Commun. Netw.-Centric Oper., Creating Inf. Force (MILCOM), vol. 1, 2001, pp. 135–138.

[5] Y. Wang, C. Hahn, and K. Sutrave, ‘‘Mobile payment security, threats, and challenges,’’ in Proc. 2nd Int. Conf. Mobile Secure Services (MobiSecServ), Feb. 2016, pp. 1– 5.