AJBMR Vol 4. Issue 3, 2023

ISSN Number (Print) – 2693-4108
ISSN Number (Online) – 2691-5103

AI based Transformation on Real Banking System 4.0

[1]Aniket Shaw, [2]Ankana Sen, [3]Arijit Das, [4]Chandrashekhar Roy, [5]Debajyoti Bhattacharjee, [6]Anwesa Das

Abstract

The comprehensive banking management system encompasses a three-tiered approach, with separate modules for administrators, bank employees, and clients. The back-end is constructed using Java Spring Boot with a layered architecture, while the front-end is built using React JS and features React Redux for state management. Token-based authentication and JPA with Hibernate as the ORM framework ensure the security and reliability of the system. An AI chatbot has been incorporated into the website to provide customer support, and a system for paperless withdrawals and deposits types transactions has been implemented to speed up banking processes. The project has determined the methodology and algorithm for introducing virtual debit cards and card- less ATM transactions for the convenience and security of customers. Additionally, the project aims to integrate data analysis into the system using AI models to analyze user spending behavior, predict efficient ATM installation locations, and implement bio- metric E-Verification processes. The focus on user-friendliness and efficiency reflects the projects goal of providing a comprehensive solution for all aspects of banking management for all parties involved.

Keywords: Physical and Digital Banking, Data Analysis, Artificial Intelligence, Machine Learning, JWT Authentication

[1]BBA Student, Institute of Engineering & Management, Kolkata, India
[2]BBA Student, Institute of Engineering & Management, Kolkata, India
[3]BBA Student, Institute of Engineering & Management, Kolkata, India
[4]BBA Student, Institute of Engineering & Management, Kolkata, India
[5]BBA Student, Institute of Engineering & Management, Kolkata, India
[6]Assistant Professor, Institute of Engineering & Management, Kolkata, India

Introduction

In today's digital world, technology has revolutionized the way we interact with financial institutions [1]. The development of a banking system management application that includes a backend built on a Relational Database Management System, a REST API constructed using the Spring Boot MVC Framework, and Spring Security, with a frontend utilizing React for UI development, API consumption, and routing, is an excellent example of how advanced technologies can be integrated to create a seamless user experience while providing robust security and data analysis. The banking system management application provides a comprehensive solution for managing transactions, account details, and user information in a structured and secure manner while utilizing the latest technologies to provide insights and improve system performance. With the large number of customers and their use of mobile and other technologies, there is an increase in transactions leading to huge amounts of data. This large amount of data presents great opportunities to the banking industry.[14] In this context, the integration of AI models for data analysis takes the banking system to the next level, enabling the system to identify patterns and trends that can help prevent fraudulent activities and optimize business operations[4- 6][11-12].

Literature Review

OTP authentication

The research paper explores the use of advanced technology to enhance online banking security and improve customer experience. Out-of-band authentication channels are proposed to provide robust protection against cyber-attacks and unauthorized access [15]. The study emphasizes the importance of user authentication and data origin authentication, such as One-Time-Passwords sent to mobile phones [2].

IDPS Method

The research also presents a new method of malicious website detection that utilizes machine learning to extract unique features from IP addresses. In addition, a network security system based on an Intrusion Detection and Prevention System (IDPS) method is proposed, which enables real-time threat detection and mitigation by sharing information on banned IP addresses and attack logs [7-9].

Biometric authentication

The study concludes that comprehensive security management that covers all aspects of the system is required to ensure effective security management. Moreover, the literature highlights the potential of biometric authentication, where unique physical or behavioral traits are used to identify individuals. The use of DNNs and CNNs is discussed, as they have proven to be effective in biometric authentication due to their ability to extract relevant features from input data and robustness to small changes [8].

Location and Spending Analysis

The training process of these algorithms is explained, and their use is emphasized in various applications such as suitable ATM location finding and spending analysis in a banking system. The literature explains the use of spatial analysis techniques such as nearest neighbor analysis and spatial clustering in finding suitable ATM locations. The use of decision tree algorithms in predicting customer spending behavior is also discussed, and the performance of the models is evaluated using various metrics. Overall, the literature emphasizes the effectiveness of advanced technology in improving online banking security, customer experience, and decision-making.

Proposed Methodology

Biometric authentication

Deep Neural Networks: Deep Neural Networks (DNNs) are a type of machine learning algorithm that are inspired by the structure and function of the human brain. They are composed of multiple interconnected layers of artificial neurons, or nodes, that process information and learn from data. DNNs can be used to solve a wide range of problems, including image classification, speech recognition, natural language processing, and generative models. The strength of DNNs lies in their ability to learn and generalize from data, allowing them to automatically extract useful features and representations from the input data. They can be trained using large amounts of data, and can learn complex, non- linear relationships between inputs and outputs [8].

Algorithm:

1. Data Preprocessing: The first step is to prepare the data for use in the network. This typically

 ISSN Number (Print) – 2693-4108
ISSN Number (Online) – 2691-5103

involves cleaning and normalizing the data, converting it into a format that can be used by the network, and splitting it into training, validation, and testing sets.

2. Architecture Design: The next step is to design the architecture of the network. This involves specifying the number of layers, the number of neurons in each layer, and the type of activation function to use in each layer.
3. Weight Initialization: The weights for the connections between the neurons must be initialized before training can begin. This is typically done using random initialization techniques.
4. Forward Propagation: During the forward propagation step, the input data is processed by passing it through the layers of the network. Each neuron in a layer takes the weighted sum of its inputs, applies the activation function, and produces an output, which is then passed as input to the next layer.
5. Loss Calculation: After the forward propagation step, the output of the network is compared to the true output, and a loss function is used to calculate the difference between the two. The loss function represents the error of the network's predictions.
6. Backpropagation: During the backpropagation step, the gradients of the loss function with respect to the weights are calculated and used to update the weights of the connections in the network.
7. Training: The training process involves repeating the forward propagation and backpropagation steps multiple times, using an optimization algorithm such as stochastic gradient descent (SGD) or Adam, until the loss reaches a minimum.
8. Evaluation: After training, the performance of the network is evaluated on the test data to assess its generalization ability.
9. Deployment: Once the network has been trained and evaluated, it can be deployed for use in real-world applications.

Convolutional Neural Networks: Convolutional Neural Networks (ConvNets or CNNs) are a category of Neural Networks that are mainly used in image recognition and processing. They are inspired by the structure and function of the visual cortex, the part of the brain responsible for processing visual information. A CNN is composed of multiple layers, including Convolutional

 ISSN Number (Print) – 2693-4108
ISSN Number (Online) – 2691-5103

Layers, ReLU (Rectified Linear Unit) Layers, Pooling Layers, and Fully Connected Layers. The Convolutional Layers perform feature detection using filters, the ReLU Layers apply an activation function to introduce non- linearity, the Pooling Layers reduce the spatial dimensions of the feature maps, and the Fully Connected Layers perform the classification [8].

Algorithm:

1. Convolution: In this step, the input image is passed through multiple filters, each of which is used to extract a specific feature from the image. The convolution operation involves multiplying the elements of the filter with the elements of the image and summing the result. This operation results in a feature map, which is a condensed representation of the input image that highlights a specific feature.
2. Activation: In this step, an activation function is applied to the feature map produced in the previous step. The activation function introduces non-linearity into the network and helps to prevent over fitting. The most commonly used activation function in CNNs is the ReLU (rectified linear unit) activation function.
3. Pooling: In this step, the feature map is down-sampled using a pooling operation, such as max pooling. The pooling operation reduces the spatial dimensions of the feature map, making the network more robust to small changes in the input image.
4. Fully Connected Layers: In this step, the features extracted from the previous steps are fed into fully connected layers, which perform the final classification. The fully connected layers contain neurons that are connected to all the neurons in the previous layer.
5. Backpropagation: The final step involves backpropagation, which is used to fine-tune the parameters of the network based on the errors made during the forward pass. This step is repeated several times until the network achieves the desired level of accuracy.

Spending Analysis

Decision trees: In the context of spending analysis in a banking system, a decision tree algorithm could be trained on data related to a customer's spending habits, such as the types of merchants they frequent, the amounts they spend, and the frequency of their transactions. The algorithm would then analyze this data and identify patterns and relationships that can be used to categorize and predict the customer's future spending behaviour [3].

Algorithm:

1. Data preparation: Gather and clean the customer transaction data, including relevant demographic information and other features that could influence spending patterns.
2. Feature selection: Choose the most relevant features to include in the model, such as age, income, location, spending category, and transaction frequency.
3. Model training: Train the decision tree algorithm on the prepared data. This involves creating a tree structure that splits the data into branches based on the most significant feature and predicts the target variable (e.g., low, medium, or high spender) at the leaf nodes.
4. Model evaluation: Evaluate the performance of the decision tree on a validation set of data, such as accuracy, precision, recall, and F1 score, to ensure that it is accurately predicting customer spending patterns.
5. Model deployment: Deploy the trained model in the banking system and use it to predict customer spending patterns for personalized financial advice and marketing.

Suitable ATM location finding for our customers using AI models

Using a location-based data analysis approach we can identify areas with a high concentration of customers and build ATMs in those areas.

Input: Customer location data, including addresses or latitude/longitude coordinates.

Output: Suitable locations for new ATMs.

A high-level methodology by which we can implement this:

1. Data Collection: Collect data on the locations of customers, including their addresses or latitude/longitude coordinates.
2. Data Cleaning: Clean and pre-process the data to remove any missing values, outliers, and irrelevant information.
3. Data Exploration: Perform exploratory data analysis to understand the patterns and relationships in the data.
4. Customer Density Calculation: Calculate the density of customers in different areas by

ISSN Number (Print) – 2693-4108
ISSN Number (Online) – 2691-5103

dividing the number of customers in each area by the area's size.

5. Visualization: Visualize the customer density on a map to help identify areas with a high concentration of customers.
6. ATM Placement: Select the areas with the highest customer density as the target locations for new ATMs.

In the data exploration step, we can also use spatial analysis techniques, such as nearest neighbor analysis and spatial clustering, to gain a deeper understanding of the distribution of customers and identify areas with a high concentration of customers.

Algorithm:

Step 1: Read the customer location data.

Step 2: Clean and pre-process the data to remove any missing values, outliers, and irrelevant information.

Step 3: Initialize a grid covering the area of interest, and assign each customer to the grid cell close to their location.

Step 4: For each grid cell, calculate the number of customers in the cell and divide it by the cell's size to obtain the customer density.

Step 5: Sort the grid cells based on their customer density in descending order.

Step 6: Select the top K cells with the highest customer density as the target locations for new ATMs.

Step 7: Output the target locations for new ATMs.

This methodology and algorithm provide a systematic and reproducible way of finding suitable locations for ATMs based on customer location data [12]. It can be easily adapted and modified to suit the specific requirements of different projects. By clearly defining the inputs and outputs, and documenting the steps involved, we can ensure that others can understand and replicate our work.

Result and Discussion

The banking industry has always been at the forefront of technological innovation, and today's banking systems are no exception. A well-designed banking system management application is critical to the success of any financial institution. This application is designed to manage banking

 ISSN Number (Print) – 2693-4108
ISSN Number (Online) – 2691-5103

transactions, account details, and user information, while ensuring that the system is secure and efficient.

The backend of the banking system management application is built on a Relational Database Management System (RDBMS). An RDBMS provides a structured way of storing data, which is critical for a banking system. The data must be stored in a manner that is easily retrievable and understandable, and an RDBMS provides this structure. Additionally, an RDBMS ensures the integrity of the data, so it is free from duplication and corruption.
REST API endpoints constructed using the Spring Boot MVC Framework is a popular way to build the backend of a banking system management application. This framework provides a comprehensive set of tools for building RESTful APIs that are efficient and scalable. The API endpoints can receive requests from the frontend, process them, and send the appropriate responses. Spring Boot is a well-documented framework, and it’s easy to get started building RESTful APIs, which is why it’s so popular.

Spring Security is a critical component of any banking system management application. Security is of the utmost importance when it comes to financial institutions. Spring Security provides a set of tools that can be used to ensure that the system is secure. These tools include user authentication, authorization, and protection against common security threats such as cross-site scripting (XSS) and cross-site request forgery (CSRF).

The frontend of the banking system management application is built using React. React is a popular frontend framework that provides a modular and reusable component-based approach to building user interfaces. The UI is built using a set of components that can be reused across the application. Additionally, React provides a mechanism for routing, which is essential for building a multi-page application. Routing ensures that users can navigate through the application in a structured and logical way.

Data analysis is an essential component of any banking system management application. AI models can be used to analyze large volumes of data quickly and identify patterns that are not visible to the human eye. This can be used to detect fraudulent activities, optimize business operations, and provide insights into customer behavior. The use of AI models can significantly improve the performance of a banking system management application.

Conclusion

The world is changing, and if we don't evolve with it, we will fall behind. The old banking systems will probably need to adopt new technologies, where the utilization of micro services increases system security. The banking system is the foundation of our economy and, in this age of cybercrime, it is crucial to have a strong system. Convenience and a rise in transaction settlement go hand in handwith robustness. Long lines at bank counters not only prolong transaction times but also adversely affect global economic growth. Long lines, staffing shortages, human error, and resource feasibility may all be addressed more effectively with digitization.

References

1. Mhlanga D. (2020). Industry 4.0 in Finance The Impact of Artificial Intelligence (AI) on Digital Financial Inclusion. International Journal of Financial Studies.
2. Panja B., Fattaleh D., Mercado M., Robinson A., & Meharia P. (2013). Cybersecurity in banking and financial sector: Security analysis of a mobile banking application. San Diego, CA, USA.
3. Gürsoy, G., & Varol, A. (2021). Risks of Digital Transformation: Review of Machine Learning Algorithms in Credit Card Fraud Detection. 2021 2nd International Informatics and Software Engineering Conference (IISEC), Istanbul, Turkey.
4. Ula, M., Ismail, Z., Sidek, M. (2011). A Framework for the Governance of Information Security in Banking System. Advanced Informatics School, Universiti Teknologi Malaysia International Campus, Kuala Lumpur, Malaysia.

5. Kochhar, K., Purohit, H., & Chutani, R. (2019). The Rise of Artificial Intelligence in Banking Sector. The 5th International Conference on Educational Research and Practice (ICERP) 2019 Educating the Digital Society – Integrating Humanistic and Scientific Values.
6. Romão, M., Costa, J., & Costa, C.J. (2019). Robotic Process Automation - A case study in the Banking Industry. 14th Iberian Conference on Information Systems and Technologies (CISTI), Coimbra, Portugal.
7. Chiba D., Tobe K., Mori T., & Goto S. (2012). Detecting Malicious Websites by Learning IP Address Features. Izmir, Turkey.
8. Ghelani D., Hua T. K., & Koduru S.K.R. (2022). Cyber Security Threats, Vulnerabilities, and Security Solutions Model in Banking. American Journal of Science and Technology.
9. Idhom M., Wahanani H. E., & Fauzi A. (2020). Network Security System on Multiple Servers Against Brute Force Attacks. Surabaya, Indonesia.
10. 10 Leo, M., Sharma, S., Maddulety, K. (2019). Machine Learning in Banking Risk Management: A Literature Review. SP Jain School of Global Management, Sydney 2127, Australia.
11. Devadevan, V. (2013). Mobile Banking in India – Issues and Challenges. International Journal of Emerging Technology and Advanced Engineering, 3(6).
12. Jakˇsiˇc, M., & Marinˇc, M. (2018). Relationship banking and information technology - the role of artificial intelligence and FinTech. Macmillan Publishers Ltd., part of Springer Nature 2018.
13. Krishna, A., Goyal, K.A., & Joshi, V. (2012). Indian Banking Industry Challenges And Opportunities. ResearchGate., Global Business and Management Research: An International Journal February 2012.
14. Bedeley, R.T., & Iyer, L.I. (2014). Big Data Opportunities and Challenges the case of Banking Industry. University of North Carolina, Greensboro. SAIS 2014 Proceedings, 2.
15. AlZomai, M., AlFayyadh, B., Jøsang, A., McCullagh, A. (2008). An Experimental Investigation of the Usability of Transaction Authorization in Online Bank Security Systems. Queensland University of Technology Brisbane, Australia.