AI-Driven Banking Security Monitoring System

Dr. P. Pavalakodi[1], Pravin Raj X[2], Rohith kumar M[3], Sabarinathan C, Sameerudeen M[5]
[1]HOD, Dept of Computer Science and Engineering
[2, 3, 4, 5] Dept of Computer Science and Engineering
[1, 2, 3, 4, 5] M.A.M College of Engineering,Tiruchirappalli, Tamil Nadu, India

Abstract- *Banking environments consistently rank among the most security-critical operational domains, where institutions must safeguard financial assets, sensitive customer information, and personnel against theft, fraud, and unauthorized access. Employees and customers operate within dynamic indoor spaces where incidents such as suspicious movement, identity concealment, or unauthorized entry may occur undetected, especially under low lighting, occlusions, and crowded conditions that conventional surveillance systems cannot reliably analyse in real time. Existing solutions — passive CCTV monitoring, rule-based motion detection, and continuous manual supervision — each fail to deliver autonomous, accurate, and real-time threat detection across complex and high-traffic banking environments. This paper introduces AI-Bank Secure, a vision-based anomaly detection and facial recognition framework purpose-built to address these limitations. The system continuously processes surveillance camera video through a motion vector-based analysis pipeline integrated with a Gaussian Mixture Model (GMM), extracting foreground segmentation, object motion patterns, and behavioural deviations to identify suspicious activities. A tracking module employing blob analysis and inter-frame object association reliably monitors movement trajectories and distinguishes abnormal behaviours such as loitering or sudden directional changes from normal customer activity. Simultaneously, an ArcFace-based deep learning model generates discriminative facial embeddings to perform real-time identity verification against a registered database.Upon confirmed detection of anomalous behaviour or unidentified individuals, multi-channel security alerts are dispatched immediately, including captured evidence frames, system notifications, and automated messages to security personnel — all without human intervention. The system operates effectively in low-light and crowded indoor conditions through adaptive preprocessing, requires no wearable devices, and maintains a structured incident log for auditing and analysis, representing a substantial advancement toward improving real-time threat detection and operational security in modern banking environments.*

Keywords: Fraud Detection, LSTM Networks, Federated Learning, Privacy-Preserving, Deep Learning

I. INTRODUCTION

Among all critical sectors, banking stands out as a highly security-sensitive environment where institutions must protect financial assets, customer data, and personnel daily. Banking spaces such as branches, ATMs, and restricted areas experience continuous activity, making them vulnerable to threats like theft, fraud, and unauthorized access. These incidents often occur under challenging conditions such as crowded environments, low lighting, and partial occlusions, were traditional surveillance systems struggle to provide reliable real-time monitoring. As financial transactions increasingly rely on digital and physical integration, the importance of intelligent and adaptive security systems has become more significant than ever.

Beyond external threats, the dynamic nature of banking operations adds complexity to surveillance. Constant movement of customers, overlapping activities, and environmental variations make it difficult to distinguish between normal and suspicious behaviour. Conventional systems relying on basic motion detection generate high false alarms and lack the intelligence to interpret complex scenarios. Similarly, traditional face recognition techniques perform poorly under variations in lighting, facial orientation, and occlusions, leading to inaccurate identification and reduced system reliability. These limitations highlight the need for more advanced and automated monitoring solutions.

The structure of modern banking environments further intensifies these challenges. Surveillance systems must monitor multiple areas simultaneously, including entrances, transaction zones, waiting halls, and secure sections. Existing methods such as manual CCTV monitoring and periodic security checks depend heavily on human attention, increasing the risk of missed incidents and delayed responses. Passive CCTV systems only record events without providing real-time analysis, limiting their effectiveness in preventing threats. As a result, critical incidents may go unnoticed until after they have occurred.

Recent advancements in artificial intelligence and computer vision provide a promising solution to these limitations. This paper presents **AI-Bank Secure**, an

intelligent surveillance framework that integrates motion-based anomaly detection using Gaussian Mixture Models (GMM), object tracking through blob analysis, and ArcFace-based facial recognition. The system enables continuous video analysis, accurate detection of suspicious activities, and automatic alert generation without human intervention. By combining behavioural analysis with identity verification, the system enhances both detection accuracy and response efficiency. The rest of the paper is organized as follows: Section II reviews related work; Section III presents the problem statement; Section IV describes the proposed system; Section V outlines system requirements; Section VI discusses implementation and results; and Section VII concludes the paper.

II. RELATED WORK

The development of intelligent surveillance systems has gained significant attention, driven primarily by the need for enhanced security in public and commercial environments such as banking institutions. Various approaches have been proposed, broadly categorized into motion-based detection, behaviour analysis, and facial recognition systems. Early studies focused on basic motion detection techniques using background subtraction and rule-based methods, which are computationally efficient but suffer from high false alarm rates and limited capability in distinguishing complex human behaviour under dynamic conditions such as crowd movement and lighting variations.

Deep learning-based approaches have been widely explored to overcome these limitations. Researchers have utilized Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and transformer-based architectures for activity recognition and anomaly detection in surveillance videos. While these models demonstrate high accuracy in controlled environments, they require large, annotated datasets and significant computational resources, making real-time deployment in practical banking systems challenging. Furthermore, their performance often degrades in scenarios involving occlusions, low illumination, and crowded scenes, which are common in real-world banking environments.

Recent advancements in facial recognition technologies, particularly deep learning-based methods such as ArcFace, have significantly improved identity verification accuracy. These systems extract discriminative facial embeddings and perform matching using similarity measures. However, their effectiveness can still be impacted by variations in pose, lighting, and partial occlusions. In addition, standalone facial recognition systems lack behavioural context, making it difficult to identify suspicious activities solely based on identity verification.

Hybrid approaches integrating anomaly detection with facial recognition have been proposed to enhance surveillance performance. Techniques such as Gaussian Mixture Models (GMM) for background subtraction combined with object tracking and behaviour analysis provide improved detection of abnormal activities. However, many existing systems either focus only on motion-based detection or rely heavily on facial recognition, lacking a unified framework that effectively combines both aspects. Moreover, several solutions depend on continuous human supervision or generate excessive false alarms, reducing their practical usability.

Across the existing literature, a clear gap remains there is a lack of efficient, real-time surveillance systems capable of simultaneously performing behaviour analysis and accurate identity recognition in complex banking environments. The proposed system, **AI-Bank Secure**, addresses this gap by integrating motion vector-based anomaly detection using GMM with ArcFace-based facial recognition, along with automated alert generation, providing a comprehensive and scalable solution for modern banking security.

III. PROBLEM STATEMENT

Therise in security threats within banking environments highlights the need for intelligent surveillance systems capable of real-time analysis. Despite extensive CCTV coverage, many incidents go undetected due to the inability of existing systems to autonomously identify suspicious activities and respond immediately.

Current solutions suffer from key limitations. Manual monitoring is prone to human error, while basic motion detection generates high false alarms and cannot distinguish complex behaviours. Traditional facial recognition methods also perform poorly under variations in lighting, occlusions, and viewing angles. Additionally, passive CCTV systems only record events without providing real-time insights, leading to delayed responses.

These limitations emphasize the need for an automated and reliable surveillance framework. The proposed system, **AI-Bank Secure**, addresses this by integrating anomaly detection, facial recognition, and real-time alert generation to improve security effectiveness in banking environments.

IV. PROPOSED SYSTEM — AI-BANK SECURE

A.System Overview

AI-Bank Secure is a non-intrusive, camera-based, fully automated surveillance system designed for banking environments. Continuous video from CCTV cameras is processed using motion analysis and machine learning techniques to detect suspicious activities. A Gaussian Mixture Model (GMM) is used for anomaly detection, while ArcFace performs real-time facial recognition. Upon detection of abnormal behaviour or unknown individuals, the system triggers instant multi-channel alerts without human intervention.

B. System Architecture

1) Data Acquisition Module:CCTV cameras capture video from key areas such as entrances and transaction zones. Frames are pre-processed using resizing, lighting adjustment, and noise reduction to ensure reliable detection.
2) Anomaly Detection Module (GMM):Each pre-processed frame is analysed using motion vector extraction and Gaussian Mixture Model (GMM) for background subtraction. The model separates moving objects from static elements and identifies abnormal motion patterns. This enables the system to detect suspicious activities such as unusual movement, loitering, or sudden behavioural deviations.
3) Object Tracking and Behaviour Analysis Module:Detected objects are grouped using blob analysis and tracked across frames using inter-frame association techniques. The system analyses movement trajectories, speed, and direction to distinguish normal activities from potentially suspicious behaviour. Persistent tracking ensures accurate monitoring even in crowded environments.
4) Facial Recognition Module (ArcFace):Faces detected within video frames are processed using the ArcFace deep learning model, which extracts high-dimensional facial embeddings. These embeddings are compared with a database of registered individuals to perform identity verification. The model maintains high accuracy under variations in lighting, pose, and partial occlusions.
5) Classification and Decision Module: Raw anomaly signals and facial recognition results are not acted upon immediately. A short temporal consistency check ensures that detected events persist across multiple frames, reducing false positives. Only validated suspicious activities or unknown identities are forwarded to the alert system.

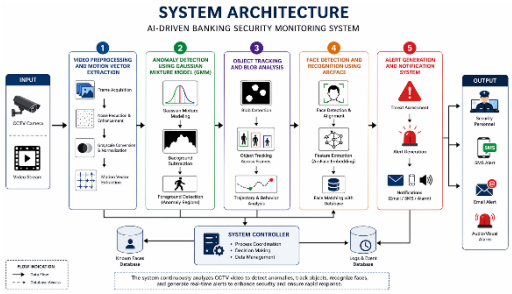

Fig. 1: AI-BankSecure System Architecture and Workflow

C. Advantages Over Existing Systems

AI-Bank Secure offers several advantages over traditional surveillance systems. First, it operates without wearable devices, ensuring ease of deployment and user compliance. Second, the integration of GMM-based anomaly detection with ArcFace facial recognition enables accurate and real-time threat identification. Third, the system supports multi-person tracking without requiring individual configuration. Fourth, multi-channel alerting ensures reliable notification even if one communication method fails. Finally, adaptive preprocessing techniques allow the system to perform effectively under challenging conditions such as low lighting, occlusions, and crowded environments.

V. SYSTEM REQUIREMENTS

Hardware requirements are modest: a dual-core processor with a minimum speed of 2.6 GHz, 4 GB RAM, and 320 GB storage are sufficient for deployment. Standard CCTV cameras are used for video input.The system is implemented using Python as the backend, with Flask for the web interface. OpenCV is used for video processing and preprocessing, while Gaussian Mixture Model (GMM) and ArcFace handle anomaly detection and facial recognition. MySQL is used for storing user data and incident logs, and HTML/CSS/JavaScript are used for the frontend. Development was carried out using PyCharm on a Windows platform. Key libraries include OpenCV, TensorFlow, Insight Face, smtplib, and requests for alert communication.

VI. IMPLEMENTATION AND RESULTSA

Dataset and Training

A. Dataset and Training

The system utilizes a combination of publicly available datasets and custom-collected CCTV footage representing real-world banking environments. The dataset includes scenarios such as normal customer activity, crowded scenes, and suspicious behaviours. Video frames are sampled

and pre-processed using resizing, noise reduction, and histogram equalization to improve quality under varying lighting conditions. Motion analysis is performed using Gaussian Mixture Model (GMM), while facial recognition is implemented using a pretrained ArcFace model.

B. Detection Results

System operates at real-time frame rates on standard hardware. Anomaly detection identifies unusual movement patterns, while ArcFace ensures accurate recognition of individuals. A short temporal consistency check is applied to reduce false positives caused by minor movements. Upon confirmation, alerts are generated instantly, including captured images and notifications sent to security personnel. All detected events are stored in a MySQL database for further analysis.

C. System Interface

The system is implemented using a Flask-based web application that provides role-based access. It includes modules such as Admin Login, User Registration, Live Monitoring Dashboard, and Incident Logs. The interface allows users to view real-time surveillance, manage data, and review detected events efficiently.

Fig. 2: AI-Bank Secure Home Page Interface

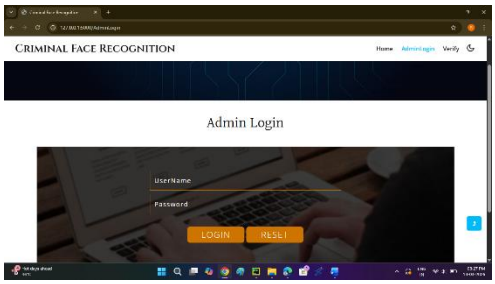

Fig. 3: Admin Login Interface

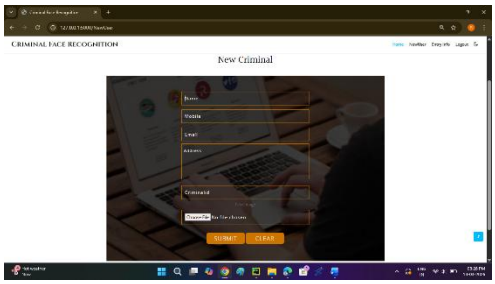

Fig. 4:New User Registration Form

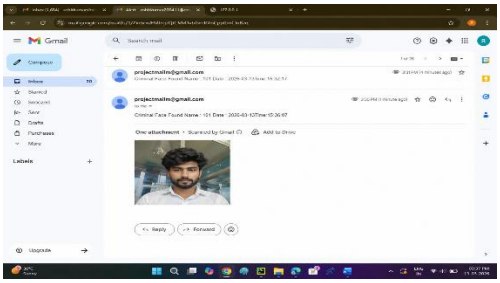

Fig. 5: Automated Alert Notification with Captured Incident Frame

The Home Page (Fig. 2) provides navigation to Admin Login, User Login, and New User Registration. Admin Login (Fig. 3) restricts system access to authorized users through secure credential verification. The New User Registration form (Fig. 4) collects user details and facial data required for identity recognition. Fig. 5 illustrates the automated alert notification sent to security personnel upon detection of suspicious activity or unknown individuals, displaying the captured image along with relevant details such as timestamp and detection status. Additional interface modules include the user dashboard for real-time monitoring and the incident log for reviewing past events.

VII. CONCLUSION

This paper has presented **AI-Bank Secure**, a real-time camera-based surveillance and threat detection framework designed to enhance security in modern banking environments. The system addresses key limitations of traditional approaches such as passive CCTV monitoring, manual supervision, and basic motion detection by enabling autonomous detection of suspicious activities and accurate identification of individuals without human intervention.The integration of Gaussian Mixture Model (GMM) for anomaly detection and ArcFace for facial recognition provides a balanced approach to improving detection accuracy while reducing false alarms. The use of temporal consistency checks ensures reliable event validation without introducing significant delays in response. The automated multi-channel alert mechanism enables immediate notification to security personnel, improving overall response efficiency. The

proposed system demonstrates a practical and scalable solution for real-world deployment in banking environments. By combining real-time behavioural analysis with robust identity verification, AI-Bank Secure represents a significant step toward improving security, reducing operational risks, and enhancing surveillance effectiveness in critical financial infrastructures.

VIII. FUTURE WORK

Planned extensions include: integration of advanced deep learning models such as Vision Transformers (ViT) for improved temporal behaviour analysis; deployment of edge computing on camera-embedded devices to enable faster processing and reduce network dependency; multi-camera integration for continuous tracking across different zones within banking environments; predictive analytics to identify suspicious behavioural patterns before incidents occur; multi-modal surveillance combining video with audio and sensor data for enhanced detection accuracy; and adaptive learning techniques to dynamically adjust detection thresholds based on environment-specific conditions.

REFERENCES

[1] Ma, Tianxiang, et al. "Abnormal behavior analysis of distribution automation system terminal based on multi-modal data fusion." International Journal of Low-Carbon Technologies 19 (2024): 2619-2625.

[2] Wastupranata, Leonard Matheus, Seong G. Kong, and Lipo Wang. "Deep learning for abnormal human behavior detection in surveillance videos A survey." Electronics 13.13 (2024): 2579.

[3] Nwakeze, Osita Miracle, Naveed Uddin Mohammed, and Nwamaka Peace Oboti. "Enhancing risk management with human factors in cybersecurity using behavioural analysis and machine learning technique." European Journal of Computer Science and Information Technology 13.51 (2025): 101-118.

[4] Jinnuo, Zhu, et al. "Analysis of existing techniques in human emotion and behavioral analysis using deep learning and machine learning models." Engineering Research Express 7.1 (2025): 012201.

[5] Vanini, Paolo, et al. "Online payment fraud: from anomaly detection to risk management." Financial Innovation 9.1 (2023): 66.

[6] Xing, Peng, and Zechao Li. "Visual anomaly detection via partition memory bank module and error estimation." IEEE Transactions on Circuits and Systems for Video Technology 33.8 (2023): 3596-3607.