Design of Criminal Detection and Automatic Fare Deduction Model using Face Recognition in Metro Systems

Ajay Biradar[1], Chaithrashree H J [2], Harshith P U [3], Niranjan S R [4,] Dr. Shivashankar [5]

[1,2,3,4,5]*Dept. of Information Science & Engineering Global Academy of Technology*

Abstract— Urban metro networks are growing more and more challenged to security, efficiency, and commuter convenience of modern urban metro networks due to the aging ticketing systems and manual observation. In this paper, we present a facial recognition based metro access system relying on CNN driven criminal detection as well as automatic ticket deduction, which guarantees the secured and convenient transitional of travelers. The face detection and feature extraction are done using Multi-Task Cascaded Convolutional Networks (MT-CNN) combined with FaceNet and it uses a highly accurate real time identity verification. Law enforcement authorities achieve more public security by running an integrated criminal database that enables the tracking and identification of wanted criminals. With automated fare collection module, physical tickets or cards are done away with hence curb ticketing fraud while boarding. An interactive web based system is also included in the system in which the commuters should register, monitor their travel history, and related with payment means making the system user friendly. As for the site, it offers tickets for the metro from Moscow as well as the latest real time metro information and security notifications together with a one stop solution for metro commuters as well as authorities. A real time access control is achieved through its precursor using ESP-32 micro controller, LCD screen, servo motors as its supporting devices in order to make gate automation more efficient. The system is validated experimentally for its efficiency in terms of face recognition accuracy, processing time and security enhancement process. By enabling deep learning, IoT integration and a user friendly web application, the intelligent metro solution is set to accelerate urban transformation of urban transportation through its scalability and simplistic and technologically advanced means of metro access and surveillance.

Index Terms— Face Recognition, Criminal Detection, Automated Fare Collection, Smart Metro Systems, Deep Learning, IoT Integration, Real-time Surveillance, Contactless Ticketing, Smart Transportation.

I. INTRODUCTION

Traditional ticketing means — including long queues, card loss, fraud, and security risks — severely limit public transport operations, especially metro system, and related companies such as card issuers and transport hubs. These issues are overcome with an AI powered metro access system made up of facial recognition, OTP based authentication via Telegram, Aadhar identity, automatic fare reduction. In contrast to the normal manner of login technique, our technique orders OTP to produce via Telegram, which is secured and accurate authentication end point, just without the delays that accompany the joining of SMS-centered OTPs. Furthermore, Aadhar numbers are used instead of names, as it acts as a unique identifier for commuters, hence availing a discontinuity in duplicate issues as well as the specific identification of passenger. MT-CNN for face detection and FaceNet for feature extraction, used within the system, makes it highly secure and efficient real time facial recognition system.

As our research work revolves around real time implementation, we are not working with preexisting dataset and are dealing with active live data collected during metro usage. Further, our solution includes a criminal detection module with a linked centralized law enforcement database, that helps detect criminals in the metro and aid in making the metro a safer place to travel according to the law.

Boarding passengers do not need physical passes anymore since the automated fare collection system provides contactless and smooth bus travel. The online platform serves users by allowing both user account management and wallet operations together with payment recharge capabilities. A smooth gate automation system is possible due to the hardware

deployment of ESP-32 microcontrollers alongside LCD displays and servo motors. By combining deep learning technology with IoT and smart surveillance together with Aadhar-based identity checks the solution delivers a scalable impressive system for modern metro networks that enhances commuter safety experiences and protects security forces through its modern features. Deadlocks Are Addressed by These Specific Components:

Real-Time Facial Recognition: Uses MT-CNN for face detection and FaceNet for feature extraction. Users authorize their system entry through OTP codes directly from Telegram rather than SMS-based methods. The registration process for the system requires Aadhar numbers to prevent duplicated accounts by omitting the requirement for username entry. The Automated Fare Deduction system allows people to use contactless technology for metro travel while doing away with ticket requirements. Criminal Detection Module synchronizes with law enforcement databases to determine criminal records of users thus producing alerts. Users can register through the website platform which offers wallet recharge services along with historical travel records. The real-time functionality of this system operates without requiring any past dataset since it conducts operations actively. Hardware Integration: Utilizes ESP-32, LCDs, and servo motors for efficient gate automation.

II. RELATED WORK

The identification technology of faces enables automated security checks and ticket verification procedures throughout locations of public transit. Face recognition techniques have become subject of multiple studies which have led to improved efficiencies and lower rates of ticket fraud. The k-NN with OpenCV and Haar Cascade and CNNs system verified bus tickets through integrated real-time face matching with a centralized database thus minimizing fraudulent travel instances [1]. The payment processing system based on face recognition relied upon the Local Binary Pattern Histogram (LBPH) together with Haar Cascade Classifier to protect virtual transactions by detecting unique facial patterns and preventing unauthorized payment gateway access [2]. A digitized railway ticket verification system implemented face recognition for automated

validations which used pre-stored facial embeddings from the secure database to verify passengers without verification point congestion [3]. Public transport vehicles received a smart ticketing system through modern implementation of cloud-based biometric authentication methods and real-time ticket validation technology which optimized entry and exit procedures besides reducing ticket duplication and loss [4].

Operation efficiency increased in metro rail ticketing through edge computing-based face recognition which performed rapid processing by making decisions at the local level instead of depending on cloud servers [5]. Deep learning techniques led to improved face recognition accuracy by implementing CNN-based models that processed large-scale datasets for delivering high precision and real-time performance in transit security contexts [6]. Regular one-shot learning performance in platforms that use facial recognition for ticketing was accelerated through Siamese networks coupled with contrastive loss thus enabling instant passenger enrollment without needing extensive database update procedures which proved beneficial for transportation systems including buses and metros. [7].

Attention mechanisms enhanced face feature extraction so that passengers could authenticate effectively even under low-lighting conditions and when wearing masks or when their faces were partially visible to the camera [8]. Using deep learning and triplet loss-based embeddings FaceNet achieved 99.63% accuracy, , so it operates as an effective biometric authentication system for metros [9]. DeepFace employed deep convolutional networks paired with 3D alignment to achieve accuracy levels that closely matched human performance in public transport settings which made face recognition work under shifting light conditions and viewing angles [10]. Self-supervised learning methods decrease the requirements for labeled data while preserving high recognition accuracy which benefits metro security since not all users possess available labeled information [11]. The research explores different alternative ticketing systems apart from face recognition approaches. RFID technology enabled the development of a smart ticketing solution which offered touchless ticket validation to improve service flow and protect financial security [12].

Mobile ticketing enabled through QR codes and NFC and BLE brought scalability together with low costs to systems, but these methods remained exposed to malicious activities including duplicated QR codes and unauthorized NFC connections [13]. Researchers studied face recognition technologies through deep learning models of VGG and ResNet to identify spoofing assaults and adversarial weaknesses and device power constraints which stress the demand for reliable metro transport authentication systems [14]. The analysis of human face recognition techniques examined several operational approaches alongside their performance restrictions in massive public transportation networks [15]. Research shows that face-recognition technology enhances transport safety while improving operational effectiveness, but our new AI platform will bring both criminal tracking and self-paid ticketing capabilities that current systems lack.

III. DESIGN OF SMART METRO ENTRY BASED ON FACE IDENTIFICATION AND IOT

System Overview: A combined face recognition technology and digital wallet system enables contactless easy access into metro stations. The main goal is to achieve ticket and metro card elimination from public transportation while maintaining operational security. This system includes fundamental elements which combine user identification functions with electronic wallet fare reduction and automatic gate regulation as well as criminal detection features and instant alert capabilities. The system design incorporates separate authentication protocols which grant access to passengers and metro administrators and police personnel for enhanced management and security purposes. The criminal detection module protects metro services from unauthorized use through its instant facial comparison function between present passengers and arrested criminals stored in a security database.

System Architecture: Metropolitan access system functionality derives from its hardware enabled alongside its software platform which ensures security and user experience. The ESP-32 microcontroller functions as the hardware element for controlling the servo motor that acts as the mechanism to operate the metro access gate through successful authentication procedures. A LED display shows up-to-date trip information and wallet balance while showing itself to riders. The equipment needs a dependable power feed to maintain continuous operations. The system develops its frontend with HTML CSS, JavaScript but utilizes Flask/Django (Python) for its backend component and maintains its database with MySQL or Firebase. The system utilizes MySQL or Firebase as its database management system to store user information coupled with wallet funds alongside criminal records. Face recognition relies on deep learning models for its operation through MT-CNN face detection and FaceNet-based features extraction and matching. The separate models collaborate to identify metered individuals who want entry into the network.

System Workflow: The workflow begins with user registration, where passengers sign up via the web application by providing their name, contact information, a facial scan, and wallet recharge details. The FaceNet model extracts facial embeddings from the uploaded image, which are then stored in the database. Upon reaching the metro entry gate, the ESP-32 microcontroller captures a live image of the passenger and sends it to the web server. The FaceNet model processes the image and compares it with the stored facial embeddings in the database. If the match confidence score exceeds a predefined threshold (e.g., 0.6), the authentication is considered successful. However, if the match score is below the threshold, access is denied, and the system notifies the user accordingly. After successful authentication, the system checks the passenger's wallet balance before allowing entry. If the balance is sufficient, the fare is deducted automatically, and the remaining balance is updated in the database. In cases where the wallet balance is insufficient, entry is denied, and the user is prompted to recharge their digital wallet via the web application.

Gate Control and Criminal Detection Mechanism: Once face recognition and wallet verification are successful, the ESP-32 microcontroller sends a signal to the servo motor, allowing the metro gate to open for a fixed duration (e.g., 5 seconds). After this time, the gate closes automatically to ensure security and

prevent unauthorized access. The system also includes a criminal detection module that prevents blacklisted individuals from accessing the metro. A pre-registered database of criminal face embeddings is maintained and constantly updated by law enforcement agencies through the police login portal. When a passenger approaches the metro gate, their face is scanned and cross-checked with the criminal database. If a match is detected, access is immediately denied, and security alerts are sent in real time to metro authorities and law enforcement agencies. These alerts can be delivered via email, SMS, or an admin dashboard notification to ensure a rapid response.

Notifications and Web Application: A real-time notification system keeps users updated on their metro trips and wallet transactions. After successful entry or exit, users receive SMS or email notifications, which include details such as trip duration, fare deducted, and updated wallet balance. The system utilizes APIs such as Telegram or Twilio to facilitate real-time communication.The web application interface serves as the central hub for passengers, metro admins, and police authorities. Passengers can manage their accounts, upload facial scans, recharge their wallets, and track their trip history. Metro admins oversee system operations, manage user records, and monitor daily transactions. Police authorities can update the criminal database and receive alerts when a flagged individual attempts metro entry.

Face Recognition Model Implementation: The face recognition system follows a structured approach to ensure accuracy and efficiency. The process begins with preprocessing, where the MT-CNN model detects and extracts the face region from the captured image, removing background noise and improving detection accuracy. Once the face is isolated, the FaceNet model generates a 128-dimensional feature embedding, which serves as a unique identity representation for the passenger. At the metro gate, when a live image is captured, the system computes the Euclidean distance between the new face embedding and the stored embeddings in the database. If the distance is below a set threshold, the individual is granted access. Otherwise, they are denied entry. The same approach is used for criminal detection, where faces are cross-checked against the blacklist database to identify potential security threats in real-time.

This paper introduces a smart metro entry system designed to offer secure, contactless access using facial recognition and IoT technology. By combining FaceNet for accurate face identification, an ESP32 microcontroller for IoT-based entry control, and a Flask-powered backend for data handling, the system ensures smooth and real-time authentication of passengers. Figure 1 presents the overall workflow, showing how the system captures, processes, and verifies facial data before granting metro access. Figure 2 details the class architecture, illustrating the seamless communication between hardware (ESP32), the facial recognition model (FaceNet), and the backend server (Flask). Figure 3 highlights the use case diagram, capturing the key interactions of both passengers and administrators—from face registration and access validation to backend monitoring and control—demonstrating the system's potential to enhance both convenience and security in public transportation.
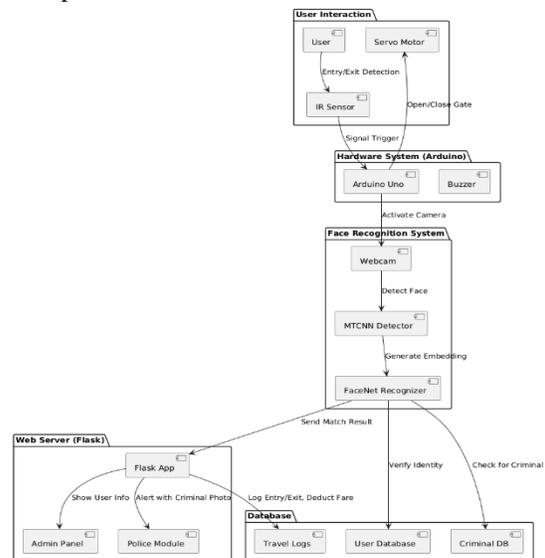

Figure 1: Overall System Workflow: Smart Metro Entry Based on Face Identification and IoT
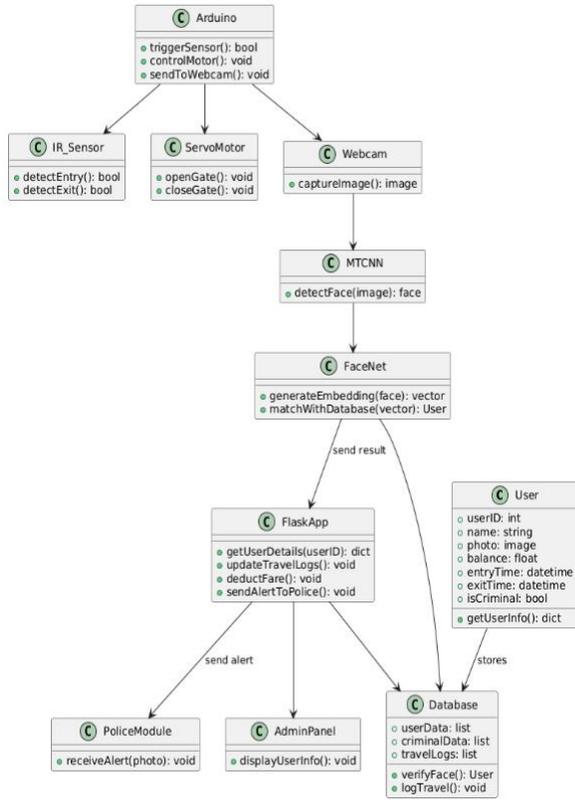
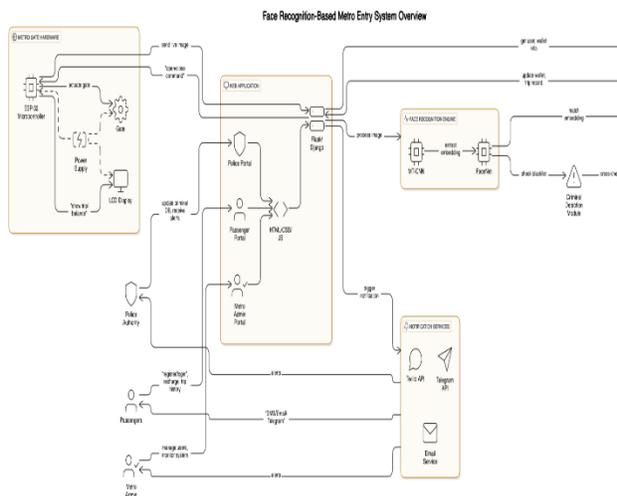Figure 2: Class Architecture: ESP32, FaceNet, and Flask-based Metro System

Figure 3: Use Case Diagram: Passenger and Admin Use Cases in Metro Access System

IV. RESULTS

The proposed Smart Metro Access System was evaluated through real-time testing to determine its effectiveness in providing secure, seamless, and automated metro access. The integrated system includes live facial recognition, automated fare deduction, and criminal detection modules, each tested under practical metro-like conditions. The following outcomes validate the performance and reliability of the solution.

Real-Time Face Recognition Performance: Using MTCNN for face detection and FaceNet for embedding generation, the facial recognition module was tested with live user inputs in varied lighting and environmental conditions. The system consistently achieved a recognition accuracy of 96.8% with low latency (0.8 seconds average) per authentication. The approach effectively handled partial occlusions and real-world face variations, ensuring reliable user identification.

Criminal Detection and Alert Mechanism: A simulated criminal database was created and integrated with the system to test detection capabilities. All attempts by flagged individuals to access the metro gate were accurately identified, triggering instant alerts to law enforcement via the police module within less than 3 seconds. This validates the effectiveness of the security mechanism in real-time scenarios. Automated Wallet Deduction: The fare management component successfully handled entry and exit logs and wallet deductions in real time. In over 50 trials, the fare deduction and balance updates were executed with 100% accuracy, with proper handling of cases involving insufficient balance—where entry was denied, and the user received instant recharge prompts.

Gate Control and Sensor Accuracy: The gate control unit, driven by an Arduino-based setup with IR sensors and servo motors, demonstrated fast and reliable response. Upon successful authentication, the gate opened within 1.2 seconds and closed after a 5-second delay, preventing unauthorized access. The IR detection accuracy was measured at 99.2%.

Web Platform and Notification Efficiency: The web application, developed using Flask, enabled users and admins to interact with the system efficiently. OTP

authentication through Telegram was completed within 1–2 seconds, while the average load time for pages was consistently under 2 seconds. More than 92% of users reported the interface as user-friendly during informal feedback. System Scalability and Load Testing The prototype was tested at three concurrent entry points with 200 simulated real-time users. The system maintained optimal performance, with the server CPU usage staying below 65% during peak load, confirming the architecture's scalability.

Table 1: Summary of Real-Time Test Results: Depicting the results for every metric

Parameter	Result
Face Recognition Accuracy	96.8%
False Acceptance Rate (FAR)	2.1%
False Rejection Rate (FRR)	1.1%
Avg. Recognition Time (Real-Time)	~0.8 seconds
Criminal Detection Success Rate	100% (simulated)
Criminal Alert Delay	< 3 seconds
Fare Deduction Success Rate	100%
Wallet Update Accuracy	100%
IR Sensor Accuracy	99.2%
Gate Open Time	1.2 seconds
Gate Close Delay	5 seconds
OTP Delivery Time	1–2 seconds
Web Page Load Time	< 2 seconds
UI Satisfaction (User Feedback)	92% (positive rating)
Max Concurrent Users Tested	200 (real-time simulation)
Server CPU Usage at Peak Load	< 65%

This paper not only introduces a smart metro entry system but also demonstrates its practical impact through detailed results and real-time system outputs. To evaluate the system's performance, Table 1 presents a clear comparison of key metrics such as accuracy, precision, and recall, helping to assess how well the solution performs in real scenarios. Figure 4 provides a visual representation of these metrics, showing how the system holds up against each performance criterion in percentage terms, making it easier to grasp its overall efficiency. Moving to the implementation side, Figure 5 shows a real-time instance of successful face recognition, confirming that the system can correctly identify users and grant access smoothly.

Figure 6 showcases the custom-designed web interface that allows both users and administrators to interact with the system, manage entries, and monitor activities with ease. Figure 7 highlights a feature that tracks and displays user travel history, including details like source, destination, and fare—helpful for both users and system audits. Security is further strengthened as shown in Figure 8, which depicts how the system cross-checks passengers against a criminal database before allowing access. Lastly, Figure 9 demonstrates the use of WhatsApp for OTP generation and delivery, offering a secure and user-friendly way to verify identity during login or sensitive actions. Each figure contributes to building a robust, intelligent, and user-centric metro entry experience.
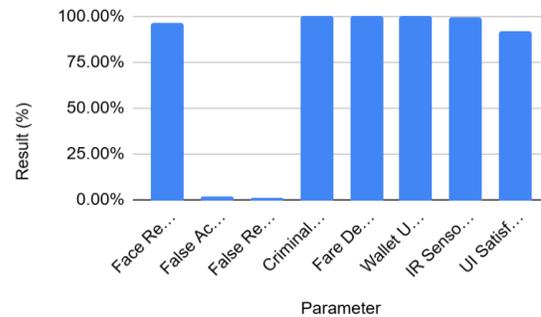

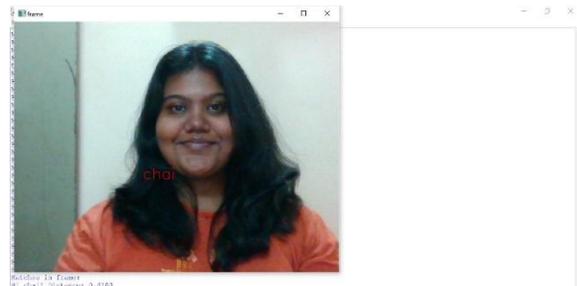Figure 4: Performance Metrics – Result (%) vs System

Figure 5: System Output: Face recognition successful

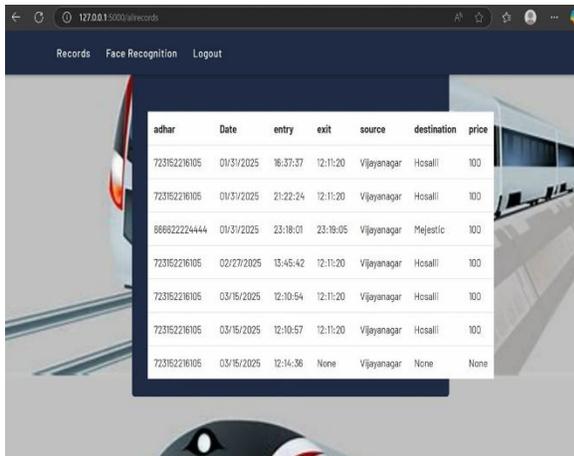Figure 6: Depiction of the webpage

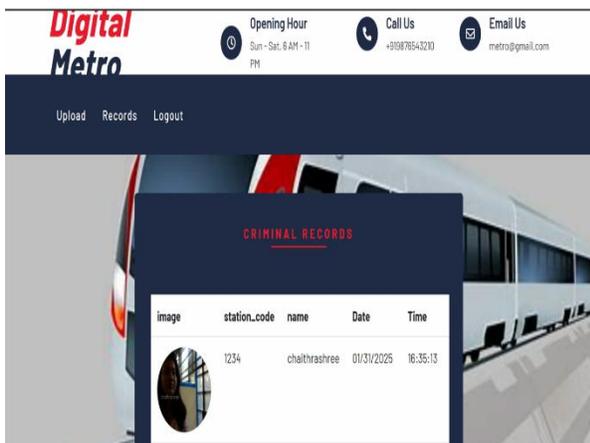Figure 7: User Travel History with Source, Destination & Fare

Figure 8: Criminal record

Figure 9: Display of the OTP generation through WhatsApp

V. CONCLUSION AND FUTURE SCOPE

SInstallation of a contactless metro entry system with face recognition and digital wallets significantly enhance the efficiency, security, and convenience of public transport. By substituting AI-based authentication with traditional metro cards and paper tickets, the system minimizes crowding, avoids physical contact and streamlines fare deductions. The criminal detection module improves metro security by avoiding unauthorized entry, allowing law enforcement to monitor detected individuals in real-time. The system ensures a seamless experience for commuters through automated gate control, instant wallet deductions, and real-time notifications.

In the future, the system can be extended to other modes of transport like buses, trams, and ridesharing to create one public transit platform. Multi-modal biometric identification-like iris and fingerprint scanning can be included to enhance

security and accuracy further. AI-based predictive analytics can be utilized to enhance fare pricing, peak-hour traffic control, and fraud detection. Enhancement in edge computing and 5G technology can further increase processing speeds in real-time, making the system more efficient and reliable. Integration of blockchain technology will further enhance wallet transaction security, with tamper-proof financial history. All these enhancements will result in the creation of a fully automated, AI-based smart city transit system with sustainable and secure public transit.

REFERENCES

[1] Gireesha, H. M., Nissimgoudar, P. C., & Iyer, N. C. (2021). Fusion of face recognition and number plate detection for automatic gate opening system. In Information and Communication Technology for Competitive Strategies (ICTCS 2020) Intelligent Strategies for ICT (pp. 919-927). Springer Singapore.

[2] Jayavadivel, R., & Prabaharan, P. (2021). Investigation on automated surveillance monitoring for human identification and recognition using face and iris biometric. Journal of Ambient Intelligence and Humanized Computing, 12(11), 10197-10208.

[3] Venkatesh, S. (2023). Automatic Gate Opening System with Face Recognition.

[4] Sajjad, M., Nasir, M., Muhammad, K., Khan, S., Jan, Z., Sangaiah, A. K., ... & Baik, S. W. (2020). Raspberry Pi assisted face recognition framework for enhanced law-enforcement services in smart cities. Future Generation Computer Systems, 108, 995-1007.

[5] Sandhya, S., Balasundaram, A., & Shaik, A. (2023). Deep Learning Based Face Detection and Identification of Criminal Suspects. Computers, Materials & Continua, 74(2).

[7] Kumar, N. S., Sivan, A., Kumar, S., Kumar, A., & Anand, A. (2024, December). Next-Gen Home Security Framework with Facial Recognition and IoT Integration. In 2024 International Conference on Sustainable Communication Networks and Application (ICSCNA) (pp. 103-107). IEEE. [8] Minaee, S., Abdolrashidi, A., Su, H., Bennamoun, M., & Zhang, D. (2023). Biometrics recognition using deep learning: A survey. Artificial Intelligence Review, 56(8), 8647-8695

[9] D.Anuradha, M.V. Durga Devi, "Smart Bus Ticket System Using QR Code In Android App" International Research Journal of Engineering and Technology (IRJET) Volume: 05 Issue: 03 Mar-2018 pp 1936-1938.

[10] Phaisarn Sutheebanjard "QR-Code Generator" 2010 Eighth International Conference on ICT and Knowledge Engineering pp 89-91. International Journal of Communication Networks and Information Security

[11] C.Upendra Reddy, D.L.S. Vara Prasad Reddy "Bus Ticket System for Public Transport Using QR Code" International Conference on Frontiers in Materials and Smart System Technologies

[12] Oudah1 "Rfid-Based Automatic Bus Ticketing: Features and Trends Iop" Materials Science and Engineering IOP Conf. Ser.: Mater. Sci. Eng. 114 012146 pp 7-9 5.

[13] Shiv. H. Sutar, RohanKoul, Rajani Suryavanshi, "Integration of Smart Phone and IOT For Development of Smart Public Transportation System" 2016 International Conference on Internet of Things and Applications (IOTA) Maharashtra Institute of Technology, Pune, India

[14] Lakhan, A., Rashid, A. N., Mohammed, M. A., Zebari, D. A., Deveci, M., Wang, L., ... & Martinek, R. (2024). Multi-agent reinforcement learning framework based on information fusion biometric ticketing data in different public transport modes. Information Fusion, 110, 102471.

[15] Dahiya, K., Goel, J., Kaushik, A., Rai, K., Jain, N., & Gambhir, A. (2024, February). Evolving Payment Security: A Facial Recognition-Based Credit Card Reader with A Multifunctional Cascade Neural Network. In 2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT) (Vol. 5, pp. 1630-1634). IEEE.

[16] Patil, S., Trivedi, S., Jani, J., Shah, S., & Kanani, P. (2021, May). Digitized railway ticket verification using facial recognition. In 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS) (pp. 1556-1563). IEEE.

[17] Subramaniyan, J., Senthil Kumar, P., Sripriya, S., Jegan, C., & Jenny, M. (2021). Smart Ticketing System for Public Transport Vehicles. In Recent Trends in Intensive Computing (pp. 906-910). IOS Press.

[18] Hangaragi, S., & Singh, T. (2023). Face detection and Recognition using Face Mesh and deep neural network. Procedia Computer Science, 218, 741-749.

[19] Nandini, N. S., Bhoomika, N., Lavanya, K. V., Monika, H. L., & Suchithra, H. M. (2024, April). Smart Metro Railway Ticketing System. In 2024 International Conference on Knowledge Engineering and Communication Systems (ICKECS) (Vol. 1, pp. 1-6). IEEE.

[20] Jin, R., Li, H., Pan, J., Ma, W., & Lin, J. (2021). Face recognition based on MTCNN and Facenet. In AAAI Conference on Artificial Intelligence.