JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

IoT-Enabled Computer Vision System for Secure and Automated Bank Locker

[1] Mrs. DIVYA M, [2]Mr.Dr.DHILIPAN J, [3]Ms.HARISHINI B ,[4]Ms. HARINI P, [5]Ms. JEEVIKA D
[1]Assistant Professor, Department of Computer Applications, SRMIST, Ramapuram Campus, Chennai
[2]Professor & Head, Department of Computer Applications, SRM IST, Ramapuram Campus, Chennai
[3,4,5]PG Students Department of Computer Applications, SRMIST, Ramapuram Campus, Chennai.

ABSTRACT:

The solution's foundation is based on an advanced biometric Multi-factor authentication (MFA) system, which is 3D facial recognition and fingerprint scanning for hardware tokenless access to bank lockers. It is the next-gen technique that comes with AI-based video analytics and Edge AI, which will catch any kind of threat instantly. This process elevates the effective rate by a margin and cuts off the overall latency time. Smart locks, enabled by the connectivity provided through the IoT, provide assurance that the blockchain systems they are connected to are competent to maintain an historical record of each access-related event-safely and endlessly. Access is also covered through role-based access control (RBAC), which provides granular permission in addition to AI-driven insights for monitoring and response of suspicious access behaviors.

The service provides highly secure quantum encryption for the cloud to better protect sensitive data today and in the quantum future. It is possible to track access event patterns across the blockchain, which gives way to immutable logging. Event-AI powered behavior analysis provides predictive alerts which proactively inform users and other authorized family members of suspicious activities in the neighborhood. This approach ensures that the systems applied in managing access to bank lockers have security, productivity, and flexibility.

Keyword: RBAC, MFA

1.INTRODUCTION:

The new system offers an innovative solution that can now be integrated to provide an elevated degree of security for the lockers of banks. This is the first example of a solution where technology is integrated with holistic security. This system uses Advanced Biometric Multi-Factor Authentication, featuring 3D face recognition, along with a fingerprint scanner, for effective and robust multi-stage user verification.

However, this system possesses the capability to not only accurately verify identities by using advanced AI algorithms but to also resist spoofing and unauthorized access. The AI-Powered Computer Vision, through integration with Edge AI, enables this system to accomplish real-time threat detection that is characterized by a remarkable speed and accuracy. High-definition surveillance cameras, nowadays equipped with advanced capabilities of AI analysis, view for unwarranted access and atypical behavior. Edge AI's use, in place of traditional cloud solutions, allows processing on-site. Therefore, it reduces latency while improving overall system performance, allowing for quick responses to potential threats.

To add further layers of security, it uses Blockchain-Based Smart Lock Management whereby each access event is logged in an incorruptible ledger. It is even supported by AI-driven behaviour Analytics, which study patterns of accessing to identify any suspicious events. Moreover, Quantum Encryption provides protection to sensitive data from future threats. Overall, such technologies form a secure yet transparent and efficient solution for managing bank locker access to bring both peace of mind and operational excellence.

2.SYSTEM ANALYSIS

2.1 Existing system:

The majority of conventional bank locker systems depend on manual verification processes. Customers are required to visit the branch in person and present their identification to gain access to the lockers. This manual methodology can be both time-consuming and inconvenient. Furthermore, it is susceptible to human error; employees may misidentify individuals or fail to adhere to established protocols, resulting in unauthorized access.

Locker systems tend to lack modern digital technologies. They lack digital monitoring and notification systems that may provide locker users with real-time alerts on access, status changes, or suspicious activities. In cases of unauthorized access or attempted breaches, locker users receive no real-time notifications or immediate alerts. Traditional systems frequently fail to have adequate backup and recovery mechanisms whenever keys are lost, misplaced, or in cases of system failure. Retrieval of access to the locker may thus require a lengthy complicated procedure, usually involving the simultaneous physical presence of both the customer and bank officials. These can be lengthy and cumbersome procedures, frustrating customers and causing operational efficiencies for banks.

2.2.PROPOSED SYSTEM:

This system proposed is a cutting-edge and complete technology solution for the security of bank lockers by means of IoT, AI-driven computer vision, and biometric authentication for the easy access, monitoring, and management of lockers. Moreover, it incorporates next-generation tools along with advanced technologies that overcome the shortcomings of traditional systems and surpass existing tools.

Key Features of the Proposed System:

1.Advanced Biometric Multi-Factor Authentication (MFA)

Facial Recognition and Fingerprint Scanning: The system employs the latest AI algorithms for facial recognition and fingerprint scanning. It requires MFA by composing multiple biometrics (face, fingerprint, or retina scan) to open the locker.

New Tool: 3D Facial Recognition. Comparing it with conventional 2D facial recognition systems, this new system contains 3D facial recognition technology that is powered by LIDAR sensors or Structured Light technologies, which have increased accuracy and provide better resistance against spoofing.

2. AI-Powered Computer Vision for Threat Detection

AI-Driven Video Analytics: AI-Driven Video Analytics: High-definition surveillance cameras, when integrated with real-time AI analysis, possess the capability to detect unauthorized access, abnormal behavior, or security threats.

New Tool : Edge AI for Real-Time Analytics. This system, unlike traditional cloud-based video processing, utilizes on-site real-time threat detection through Edge AI to reduce latency and maximize performance. Advanced models such as YOLOv8 and Deep Stream SDK are used for object detection as well as behavior analysis.

3. Smart Lock with IoT Connectivity

Advanced IoT Smart Lock: The advanced Internet of Things (IoT) smart lock utilizes either Wi-Fi 6 or LORAWAN technology, enabling it to provide real-time data transmission while ensuring enhanced security.

New Tool: Blockchain-Based Smart Lock Management. This innovative tool replaces traditional access logs with blockchain technology, thus ensuring that each locker access event is cryptographically secure and tamper-proof and fully transparent. Blockchain-based systems do not allow unauthorized access or data tampering and will create an immutable record of all locker activities.

4. Family Data Management and Role-Based Access Control (RBAC)

Role-Based Permissions: he locker owner can provide family members with role-based access to the locker, thereby differentiating these access permissions - for example, viewing logs in the locker, opening the locker, and changing or removing surveillance footage.

New Tool: AI-Powered Access Insights. This feature leverages the strength of machine learning algorithms in understanding patterns in access, providing security insight. In the event that the system detects abnormal access patterns, such as multiple attempts at unusual hours, it automatically issues alerts to the owner and family members.

5.Cloud-Based Data Management with Quantum Encryption

Cloud Integration: All logs, biometric data, and video recordings related to surveillance are stored securely in the cloud. This way, users can view their locker history in real-time.

New Tool: Quantum Encryption replaces traditional AES encryption with quantum encryption techniques, which provide future-proof security as it now guards sensitive data against every possible threat posed by a quantum computer, thus ensuring both data stored and information in transit remains secure.

6. User Visit History Logging and Analytics

Blockchain for Immutable Logs: In order to guarantee tamper-proof logging of locker access, a blockchain-based logging system may be utilized, wherein each access is securely recorded on a distributed ledger. Platforms such as Hyperledger Fabric or Ethereum could be employed.

AI-Driven Behavior Analytics:It involves the use of tools like Scikit-learn and TensorFlow, which have machine learning capabilities, to analyze access patterns and detect any anomaly or suspicious activity.
Real-Time Alerts: AI models identify access anomalies, like attempts outside usual hours, and trigger instant alerts via the mobile app or SMS.

7. Real-Time Alerts and Emergency Access

New Tool: AI-Enhanced Predictive Alerts The system uses predictive analytics to detect abnormal patterns of access or suspicious activities, which could prompt immediate alerts proactively to both the locker owner and authorized members of his household. It reduces false alarms as contextual information and user behavior may be analyzed immediately.

Secure Access in Emergency: Access for authorized family members can be given during emergencies with multi-factor authentication based on biometric and passcode-based.

.3. System Architecture

The architectural structure of this system will integrate several layers which include IoT, cloud, edge computing as well as AI to deliver enhanced security and user experience.

3.1 IoT and Hardware Layer

3D Facial Recognition Hardware:

Edge AI Smart Cameras: Equipped with real-time analytics capabilities, these cameras use Edge AI (with NVIDIA Jetson or Google Coral chips) to process surveillance footage locally, reducing the need for constant cloud transmission.

Blockchain-Enabled Smart Lock: The locker's smart lock integrates with a blockchain ledger, ensuring an immutable record of every access attempt and ensuring data integrity.

3.2. Processing and AI Layer

Edge AI Models: Advanced artificial intelligence models, such as YOLOv8 for object detection and the Deep Stream SDK for real-time behavior analysis, are implemented on edge devices to facilitate rapid, low-latency decision-making.

Machine Learning-Based Access Pattern Analysis: It will closely monitor the locker access pattern and identify anomalies such as unauthorized attempts and suspicious behaviors, raising alarm in advance.

3.3 Cloud and Data Security Layer

Cloud Storage: Access logs for lockers, surveillance footage, and biometric data are securely stored within a cloud environment, thereby guaranteeing remote access and backup.

Quantum Encryption: Data in transit and at rest is secured using quantum cryptographic algorithms that are resistant against attacks by potential future quantum computers.

Blockchain Ledger: The blockchain ledger serves as a repository for access logs and biometric data, thereby offering a decentralized and tamper-proof account of locker activities.

3.4 User Interaction Layer

Mobile and Web Application Interface: An interface designed for user-friendliness enables locker owners and authorized family members to efficiently manage access, observe real-time footage, and receive notifications. The application is developed utilizing React Native or Flutter for mobile platforms, and React.js for web platforms.

3.5. AI-Driven Alerts and Reports:

The application equips users with predictive warnings and locker usage-related security insights and periodic reports. On top of that, users can view live videos from the smart cameras.

3.6. Application Layer (User Interface & Management)

The application layer provides users and system administrators with access to overall functionality, namely - locker control, history logging, and family data management.

Mobile/Web Application (for Users):

User Authentication: Uses multi-factor authentication (MFA) such as SMS**,** email**,** or Authenticator App (e.g., Google Authenticator) for secure login.

Locker Access Control:

Remote Unlocking: Users can unlock lockers remotely via the mobile app.

Real-Time Alerts: Users receive notifications when their locker is accessed or if tampering is detected.

Family Data Management:

Manage Family Access: Authorize, modify, or revoke family members' access to lockers.

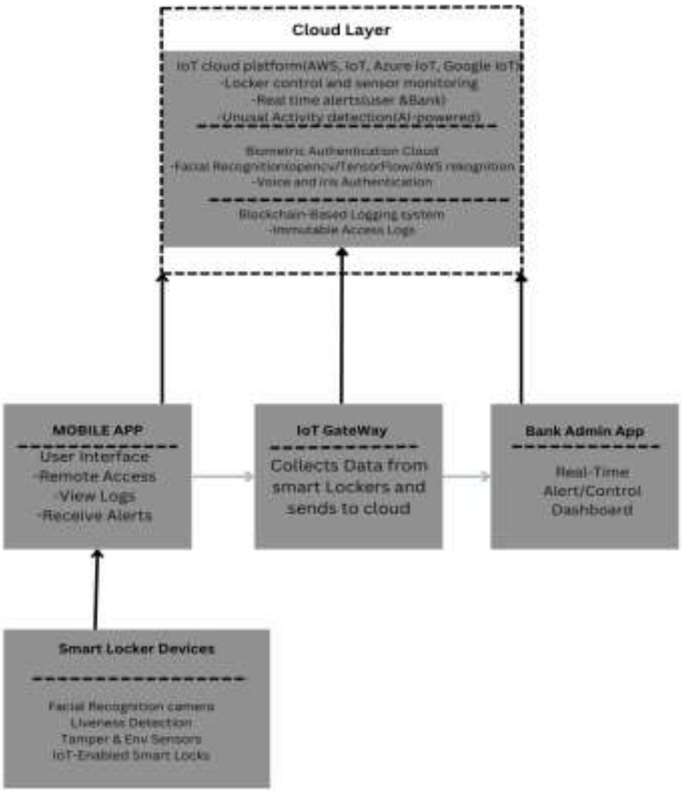
Temporary Access Creation: Generate temporary access tokens or PINs for emergency use.

View Access History: Shows detailed logs of who accessed the locker and when, along with sensor data.

Mobile/Web Application (for Bank Staff):

Administrative Dashboard: Monitor locker activity and user management.

Override Controls: Bank administrators can unlock lockers during emergencies, with multi-level authorization.


Cloud Layer
IoT cloud platform(AWS, IoT, Azure IoT, Google IoT)
-Locker control and sensor monitoring
-Real time alerts(user &Bank)
-Unusal Activity detection(AI-powered)
Biometric Authentication Cloud
-Facial Recognition(opencv/TensorFlow/AWS recognition
-Voice and iris Authentication
Blockchain-Based Logging system
-Immutable Access Logs
MOBILE APP
User Interface
-Remote Access
-View Logs
-Receive Alerts
IoT GateWay
Collects Data from smart Lockers and sends to cloud
Bank Admin App
Real-Time Alert/Control Dashboard
Smart Locker Devices
Facial Recognition camera
Liveness Detection
Tamper & Env Sensors
IoT-Enabled Smart Locks

[Architecture diagram]

4. SCOPE OF THE PROJECT:

The aim of this project is to design, develop, and implement a high-end bank locker management system that integrates advanced technologies to ensure both security and efficiency. One of the central features of this project is the incorporation of Multi-Factor Authentication (MFA). In this case, 3D facial recognition is combined with fingerprint scanning in order to provide a highly secure authentication process. The 3D facial recognition technique further improves user verification accuracy while also providing resistance to spoofing attempts through the application of LIDAR and Structured Light technologies. A further critical component of the project is the AI-driven threat detection systems. With the use of high-definition surveillance cameras and Edge AI, the solution shall be able to perform real-time video analytics and on-site threat detection. This approach cuts latency and enhances performance much more than a typical solution based on the cloud. Advanced AI models that involve object and behavioral analysis, such as YOLOv8 and Deep Stream SDK, shall be utilised for the detailed detection of objects and rapid identification of possible security risks. The development also focuses on the smart lock technology as well, including enhanced IoT connectivity.

The system will allow for real-time data transmit while providing improved security management by using the Wi-Fi 6 or LORAWAN-enabled smart locks. Blockchain technology incorporated for the management of smart locks will ensure an immutable record of access events, therefore, providing integrity and transparency with data. Additionally, the system will incorporate RBAC in the management of family data to provide varied kinds of access permission based on a user's role and offer AI-driven insights about access patterns.

Data management in the system shall be cloud-based with safe storage of access logs, biometric data and surveillance footage. This data will also be protected by quantum encryption techniques to secure it from possible quantum computing attacks in the future. The project will also implement blockchain technology to achieve immutable logging of access events and AI-driven behavior analytics that can identify unusual activities and send real-time alerts. Finally, the system will include AI-based predictive notifications aimed at actively pinpointing possible security breaches and sending notifications to both the user and bank officials. For any crisis situation, access mechanisms for emergency will be provided that allow authorized users to gain temporary access through multi-layered verification processes

5. ALGORITHM FOR IOT-ENABLED COMPUTER VISION SYSTEM

5.1. Initialization and System Setup

Initialize IoT Devices:

Connect cameras, sensors (e.g., motion detectors), and actuators (e.g., electronic locks) to the network.

Ensure all devices are properly configured and communicate with a central server or gateway.

Load Pre-trained Models:

Load machine learning models for face recognition and object detection from storage.

5.2. Data Collection and Preprocessing

Capture Data:

Video Feed: Continuously capture video from surveillance cameras.

Sensor Data: Collect input from motion sensors and other relevant IoT devices.

Preprocess Data:

Image Preprocessing: Convert captured images to grayscale, normalize, and resize as needed.

Noise Reduction: Apply filters to reduce noise and improve image quality.

5.3. Face Detection and Recognition

Face Detection:

Use a face detection algorithm (e.g., Haar cascades, YOLO) to locate faces in the video feed.

Face Recognition:

Extract facial features using a deep learning model (e.g., Face Net, a custom CNN).

Compare extracted features with those in the database to identify individuals.

Access Control Decision:

If the recognized face matches an authorized user, grant access.

If the face does not match, deny access and trigger an alert.

5.4. Automated Locker Access

Decision Making:

Based on the face recognition result, decide whether to unlock the locker.

Control Locker:

Send a command to the electronic lock to either open or remain locked based on the decision.

5.5. Real-Time Surveillance and Anomaly Detection

Motion Detection:

Use motion detection algorithms (e.g., frame differencing, background subtraction) to identify unusual activity.

Anomaly Detection:

Implement algorithms to detect unusual patterns or behaviour (e.g., multiple attempts to access, prolonged presence near the locker).

Event Logging:

Log detected anomalies and events (e.g., unauthorized access attempts, system errors) in a secure database.

5.6. Data Management and Storage

Aggregate Data:

Collect and aggregate data from video feeds, sensor inputs, and access logs.

Secure Storage:

Store aggregated data in a secure database, ensuring encryption and access control.

Data Analysis:

Analyze stored data for patterns and trends (e.g., frequent access times, unauthorized access attempts).

Generate reports and alerts based on the analysis.

5.7. User Notifications and Alerts

Generate Alerts:

Automatically generate alerts for administrators in case of anomalies or unauthorized access attempts.

Send Notifications:

Deliver notifications via email, SMS, or a mobile application.

5.8. System Maintenance and Updates

Regular Updates:

Periodically update the computer vision models and IoT device firmware.

Performance Monitoring:

Continuously monitor system performance and functionality, making adjustments as needed.

Fig (a) hardware components.

Fig (b) Modern Bank Locker System.

6. FUTURE ENHANCEMENT:

Future improvement unborn advancements for the IoT- enabled bank locker operation system can greatly enhance its functionality, security, & stoner experience. One major upgrade could be adding further biometric options. These might include voice recognition, tone pattern analysis, and gait discovery. similar updates would add further layers of security to the formerly strongmulti-factor authentication system. AI-powered prophetic conservation is another crucial point. IoT detectors would keep an eye on smart cinch health & other vital factors. They would prognosticate issues before they be, enabling smooth service and lower time-out for druggies. also, using 5G technology could help speed up communication between the IoT bias & the pall. This would lower quiescence for real- time monitoring, briskly trouble discovery, & hastily alert announcements. Another instigative upgrade involves using AI to dissect stoner geste

patterns. This system can spot implicit fraud beyond traditional security measures. For data security, enforcing amount-safe blockchain tech could cover pivotal access logs from any pitfalls posed by amount computing. It would insure that these logs remain secure in the long run. also, stoked reality(AR) could play a part in perfecting stoner experience. It might give visual tips or step- by- step backing for managing lockers, making everything easier for druggies. The system could also have automatic exigency response features that work with original law enforcement or bank security during critical situations. This would allow for quicker responses when demanded most. farther integration with smart sidekicks like Alexa or Google Assistant could allow druggies to control locker access and check security logs with just their voices. This makes relations smoother and further intuitive. sequestration- Conserving AI models like allied literacy may also be employed. These models process sensitive data locally, which helps ameliorate sequestration by reducing the need to shoot biometric information to other waiters. Incipiently, expanding the system so that druggies can pierce lockers at different branches while being connected to a central account could give indeed more convenience without immolating strong security — especially for those who frequently visit colorful bank locales.

7. CONCLUSION

In summary, the bank locker operation system which is supported by IoT results is a good development in minimizing pitfalls & perfecting robotization of access to bank lockers. egregious developments include using AI grounded biometric, unresistant blockchain log and nearly unbreakable amount encryption. In addition to these security measures which are simple to understand, there's an AI backed videotape analytics system that together with Edge AI looks out for and even cautions them of any pitfalls in real time. thus placing smart cinches using conventional styles has a decent functional operation but does n't offer any form of fresh protection against unauthorised use except for a dated log of who penetrated the smart cinches which is again veritably questionable in terms of responsibility and safety. In addition, surveillance and engagement systems enforced within the system support part- grounded access control & family data operation. This makes warrants flexible because only people approved by the system director are allowed to use important features. But still possible problems similar as unusual stoner's exertion are avoided since there are also exigency access options and smart AI cautions. With further guests coming to banks with complicated security issues, this system comes as a total remedy to the current challenges while situating itself for unborn advancements like amount evidence cryptography and AI grounded prophetic conservation. This guarantees that it'll continue to be reliable & secure in the long run.

8. REFERENCES

1. Zhang, D., & Li, Y.(2018). Handbook of Facial Recognition. Springer. - This book provides an overview of facial recognition technologies, including advanced biometrics like 3D facial recognition.

2. Redmon, J., & Farhadi, A.(2018). YOLOv3 An Incremental improvement. arXiv preprint arXiv 1804.02767. - Discusses YOLOv3, an advanced object discovery model used in AI- driven video analytics for real- time trouble discovery.

3. Nakamoto, S.(2008). Bitcoin A Peer- to- Peer Electronic cash system https// bitcoin.org/bitcoin.pdf. - The original paper on blockchain technology, which is foundational for blockchain- predicated smart ice operation and access logs.

4. Gisin, N., Ribordy, G., Tualle- Brouri, R., & Grangier, P.(2002). Quantum Cryptography. Reviews of modern medicines, 74(1), 145. - This paper discusses quantum cryptography ways that are critical for securing data against future quantum calculating risks.

5. Chandola, V., Banerjee, A., & Kumar, V.(2009). Anomaly Detection A Survey. ACM Computing checks(CSUR), 41(3), 1- 58. - A comprehensive check on anomaly discovery ways, applicable for AI- driven behavior analytics in trouble discovery.

6. Bertino, E., Sandhu, R.(2005). part- predicated Access Control AMulti- Dimensional View. Proceedings of the 10th ACM Symposium on Access Control Models and Technologies. ACM. - This paper discusses part- predicated access control, vital for managing locker access and family data operation.

7. Pereira, P. P., & Aguiar, R. L.(2021). IoT Security Advances in Authentication and Encryption ways. International Conference on Information Systems Security and insulation(ICISSP), 2021. - Provides perceptivity into IoT security, fastening on advanced authentication mechanisms and encryption ways in smart systems.

8. Huang, C., Ding, Z., & Fan, P.(2019). Edge AI Vision, Challenges, and future Directions. Proceedings of the IEEE International Conference on Dispatches(ICC), 2019. - This paper explores the eventuality of Edge AI for real- time processing and analytics, which is vital for reducing quiescence in trouble discovery.

9. Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L.(2016). Edge Computing Vision and Challenges. IEEE Internet of goods Journal, 3(5), 637- 646. - Discusses the advantages and challenges of edge computing, which is a vital element in AI- powered computer vision systems for real- time analytics.

10. Puthal, D., Sahoo, B., & Mohanty, S. P.(2018). Blockchain for Secure Cloud- Based Data Management in IoT Systems. IEEE International Conference on Cloud Computing, 2018. - This conference paper discusses the operation of blockchain in secure data operation for IoT, which is pivotal to the blockchain- predicated smart ice operation system.

11. Deng, L., & Li, X.(2020). Quantum- Safe Cryptography for Cloud and IoT Systems. IEEE International Conference on Cloud Computing Technology and Science(CloudCom), 2020. - Examines the performance of quantum-safe encryption ways in pall and IoT surroundings, aligning with the quantum encryption point of the system.