International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 11 Issue: 12 | Dec 2024 www.irjet.net p-ISSN: 2395-0072

Bank Locker Security System Using Machine Learning

Samiksha Wagaj[1], Vaishnavi Gund[2], Sonali Mane[3], Divya Sapkal[4], prof.I.Y.Inamdar[5], Prof.S.D.Pandhare[6]

[1]Student, Dept. of Computer Science & Eng., SMSMPITR, Akluj, Mharashtra, India
[2]Student, Dept. of Computer Science & Eng., SMSMPITR, Akluj, Mharashtra, India
[3]Student, Dept of Computer Science & Eng., SMSMPITR, Akluj, Mharashtra, India
[4]Student, Dept of Computer Science & Eng., SMSMPITR, Akluj, Mharashta, India
[5]Professor, Dept. of Computer Science & Eng., SMSMPITR, Akluj, Mharashtra, India
[6]Head of Department, Dept. of Computer Science & Eng., SMSMPITR, Akluj, Mharashtra, India

---

Abstract - *This research proposes a robust bank locker security system integrating machine learning with face detection and OTP authentication. The system utilizes a state-of-the-art face recognition algorithm to accurately identify authorized users, ensuring that only legitimate individuals can access their lockers. This research is used for bank because when the customer comes to bank to deposit his valuables in the bank locker for the security of the locker and we have used face recognition and one time password through machine learning to check whether the customer who came is real or not. Using face recognition for bank locker security has made it easier to identify authorized persons, Because we have used two factor authentication i.e. one time password message is sent to the authorized person's phone so high security is for bank lockers. Bank locker security using machine learning with face detection and OTP authentication it is very useful for bank and high security for bank lockers.*

Key Words: Face Detection, OTP Authentication, Machine Learning, etc.

1.INTRODUCTION

The In recent years, the importance of security in banking and financial institutions has escalated, with physical and digital threats evolving in complexity. A critical component of bank security is the protection of locker systems, which store valuable items such as documents, jewelry, and other assets. Traditional methods of accessing these lockers, such as physical keys or PIN-based systems, can be vulnerable to theft, human error, or unauthorized access. As a result, the banking sector is increasingly looking toward more advanced technologies, such as machine learning, biometrics, and multi-factor authentication (MFA), to enhance the security of their locker systems. One such innovative approach is the integration of face detection technology with One-Time Password (OTP) authentication, powered by machine learning.[1].This combined approach aims to provide a robust, user-friendly, and highly secure system for accessing bank lockers. Bank locker security is a critical component of modern financial institutions, as it protects valuable assets and confidential documents from theft and unauthorized access. Traditional security systems, relying on physical locks, keys, and surveillance cameras, are becoming increasingly vulnerable to sophisticated security threats and human error. To address these challenges, machine learning (ML) has emerged as a promising solution to enhance and automate locker security. By leveraging ML algorithms, banks can develop intelligent systems capable of detecting anomalies, recognizing patterns in access behavior, and even predicting potential security breaches before they occur. [2]. Bank locker security is a critical aspect of safeguarding valuable assets and sensitive documents stored by customers in financial institutions. Traditional security measures, such as PIN codes, passwords, and physical keys, have proven to be vulnerable to various types of attacks, including unauthorized access, fraud, and social engineering. In light of these challenges, integrating machine learning (ML), face detection, and OTP (One-Time Password) authentication offers a robust and multi-layered security approach that significantly enhances the protection of bank lockers. [3]. By incorporating face detection, banks can leverage biometric authentication, ensuring that only authorized users gain access to lockers based on the unique features of their faces. This biometric factor provides a highly secure method of user identification, minimizing the risks associated with stolen credentials or impersonation attempts. Additionally, OTP authentication introduces a second layer of protection by verifying that the individual attempting access has the correct time-sensitive code sent to their registered mobile device or email. [4]. Through machine learning, the system can continuously learn user behavior patterns, detect anomalies in real-time, and adapt to evolving security threats. For example, ML models can identify abnormal login attempts, flag suspicious behaviors such as multiple failed authentication attempts, or recognize attempts to access the locker from unusual locations or devices. [5].

1.1 Literature Review

Ref. no.	Paper Name	Author Name	Method
1	Locker Security System Using Facial Recognition and One Time Password (OTP)	N. Anusha, A. Darshan Sai and B. Srikar	The proposed locker security system aims to address current security issues by integrating IoT (Internet of Things), face recognition, and OTP (One-Time Password) technology. To access the locker, users must enter a pre-set PIN, ensuring secure authentication before access.
2	Bank Locker Security System using Machine Learning	Right Yogesh Kumar, Vinay Dogra	This project proposes a bank locker security system that utilizes machine learning for face and liveness detection. By combining computer vision and machine learning algorithms, the system accurately identifies the individual attempting to access the locker and verifies their identity to ensure secure access.
3	Bank Locker Security System Using Machine Learning with Face and At the same time, we Liveness Detection	Priti Kandekar1, Aishwarya Pisare1, Rupali Margale1	This paper presents the design and implementation of a bank locker security system that grants access only to individuals whose faces are registered in the training database. The system begins by detecting human motion, followed by face recognition to verify the individual's identity. The coordinates of the detected motion are tracked, and if the face cannot be recognized, the system automatically passes the coordinates to an anesthetic gun to target the intruder.
4	An IoT based Bank Locker Security System	J. Thirumalai , Gokul. R, Manellore Murali. M ,Jackson Jublience	This paper focuses on developing an effective, self-operating security system for bank locker rooms. In the event of a robbery, unauthorized access to the locker room area can be detected by the proposed system. Traditional human-operated security systems often fail to identify robbers due to a lack of evidence. However, the development of advanced sensors has allowed for more proactive security measures. To address the protection of sensitive documents and valuable items, the paper proposes an Automated Safety Vault with a Double Layered Defense Mechanism, offering enhanced security for critical assets.
5	Bank Locker Security System using Machine Learning with Face and	Single line spacing Prof. Sunil M. Kale, Anuja Nair, Manasi Pagar,	One of the major challenges facing financial systems today is ensuring the security of

	Liveliness Detection	Esha Kamble	transactions. To address this, banks worldwide are increasingly adopting biometric authentication, as it is both convenient and widely accepted. In offline settings, facial recognition is often used to match digital selfies with ID document photos, and similar technologies are employed in automatic immigration controls. However, a key challenge is minimizing discrepancies between facial images from different sources. To tackle this issue, we propose a unique architecture that leverages deep features extracted using two well-established convolutional neural networks (CNNs) for cross-domain facial matching. Data from the Face Bank collection demonstrates that this approach effectively addresses the face-to-face comparison problem, achieving over 93% accuracy. The results suggest that this method should be integrated into real-world banking security systems for enhanced protection.

6	HIGH PROTECTION VOICE IDENTIFICATION BASED BANK LOCKER SECURITY SYSTEM WITH LIVE IMAGE AUTHENTICATION	G. VIJAYA LAKSHMI, M. KIRANMAI	As human civilization advanced, the need to secure valuable assets such as money, property, and jewelry became increasingly important. People began to store their valuables in bank lockers for safekeeping. However, incidents of fraud, where unauthorized individuals access lockers and steal valuables, still occur. To address this security threat, it is crucial to authenticate the identity of individuals who wish to access a locker. To enhance security, a system has been proposed that combines voice identification, face detection, and GSM technology, ensuring that only authorized users can access the locker.
7	IoT Based Bank Locker System using OTP Technology	Dr. Sheeja V Francis,2 Rupus Daniel J,3 Sarath K, 4 Surendar N, 5 Sathish Kumar S.	This paper proposes a secure bank locker system based on Fingerprint and OTP (One-Time Password) technology, designed for use in banks, offices, and homes. The system ensures that only authenticated individuals can access their stored documents or money. Initially, users must register their username, password, and

			mobile number in an authorized database. Once the username and password are verified, the person's fingerprint is captured and stored with a unique ID. If the fingerprint matches the stored ID, a four-digit OTP is sent to the user's mobile phone, which is required to unlock the locker. Additionally, the system can maintain a log of check-in and check-out details for each user, along with basic information for enhanced tracking and security.
8	Bank Locker Authentication System using Facial Recognition	Yash D. Satare,Saurabh Y Girme,Sagar Walunj	Security and authentication are crucial in daily life, especially for accessing bank lockers. This paper proposes a smart digital door lock system for bank automation that uses digital information, including user data and face recognition, for authentication. In this system, banks store face imprints of individuals for locker access, ensuring only authorized users can retrieve money or documents. The system employs a Convolutional Neural Network (CNN) algorithm for facial recognition. However, facial recognition alone is not enough to verify authenticity, as it cannot confirm whether the person is real or a spoof. To address this, liveness detection is implemented. The system uses eye blink detection as part of the liveness detection process, ensuring that the person interacting with the system is live, not a photo or other fake artifact.
9	BANK LOCKER SECURITY SYSTEM USING FACE RECOGNITION AND LIVELINESS DETECTION	Dr. Poonam Lambhate1 Aarshin Inamdar2, Rucha Gaikwad3, Vaishanavi Madane4, Mayuri Khedkar5,	The current work presents the development of a smart locker system for the banking industry. A key feature of this system allows users to check whether their facial expressions are normal before accessing the locker. The smart lock application compares the user's face to the data stored in the database. If the face appears abnormal or unfamiliar, the locker will remain locked. This process of identifying known or unknown faces is referred to as face recognition. The goal of the system is to create a hybrid biometric authentication method that does not rely on specific biometric hardware, ensuring flexibility and security for users.
10	Bank Locker	Akash Mote1 ,	Ensuring the

	Security System using Machine Learning with Face and Liveness Detection	Kanhaiya Patil1 , Akshay Chavan1 , Mrunal Saraf1 , Prof. Ashwini Pandagale2	security of transactions is a major challenge facing banking systems today. Biometric authentication, particularly facial recognition, is gaining widespread adoption due to its convenience and effectiveness, with banks investing heavily in these technologies. In offline environments, face images from ID documents are often compared to digital selfies, and this approach is also used in broader applications, such as automatic immigration control. However, a significant challenge arises from the differences between facial images, which may come from various sources, such as ID photos and selfies. To address this challenge, we propose a novel architecture for cross-domain facial matching, leveraging deep features extracted by two well-established Convolutional Neural Networks (CNNs). Results from a dataset called "Face Bank" demonstrate that the proposed method achieves over 93% accuracy in face-to-face comparisons. This high accuracy highlights the potential of the approach for inclusion in real-world banking security systems, enhancing the reliability and security of identity verification processes.

1.2 Problem Statement

This research proposes a hybrid authentication system combining face recognition and OTP verification to overcome the limitiations of traditional systems, offering higher security, reliability, and ease of use.

1.2 Scope

The scope of bank locker security using machine learning with face detection and OTP authentication includes enhanced multi-layered security. Machine learning models improve system adaptability by learning user behavior patterns, providing robust protection against unauthorized access. Additionally, this system ensures compliance with regulatory standards while offering scalability and customization for different security needs.

1.3 Objective

This system aims to enhance traditional security measures by incorporating multi-factor authentication techniques. By leveraging machine learning algorithms for face detection and integrating One-Time Password (OTP) verification, the system will provide a high level of accuracy, convenience, and safety for locker access in banking environments.

2. The Proposed Work

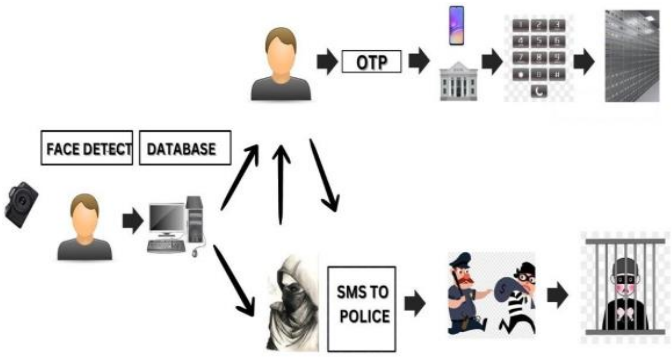

Fig -1: System Architecture

User: The most essential part of system is its user. Firstly, user register their facial data along with their necessary details.

Face detection: Compare the detected face with stored facial data of authorized users. If a match is found to OTP generation; otherwise, access is denied.

OTP Authentication: Once the users face is recognized, an OTP is sent to the registered mobile number.

Locker access: Once the user is authorized then accessing the easily locker.

2.1 Face Detection:

Fig -2: Face Detection

Face detection using machine learning is a fundamental task in computer vision that involves identifying and locating human faces within images or videos. It's a critical technology in applications like facial recognition, security systems, photo tagging, and augmented reality. Here's an overview of how face detection works, key techniques, and popular machine learning algorithms used in this task. Face detection aims to find the location of one or more human faces in an image or video stream. The key challenge is distinguishing faces from other objects and backgrounds, even when they are partially occluded, appear at different angles, or have various lighting conditions.

2.2 OTP Authentication:

Fig -3: OTP Authentication

OTP (One-Time Password) Authentication is a security mechanism that generates a unique password for a single use, enhancing the security of user accounts. It is typically used as part of two-factor authentication (2FA**)** systems, where the user must provide both something they know (e.g., a password) and something they have (e.g., an OTP sent via SMS, email,). OTPs are usually valid for a limited time or a single session, which provides an added layer of security.

3.3 Bank Locker:

Fig -4: Bank Locker

Once the user is authorized then accessing the easily locker. A bank locker is a secure, private storage space within a bank or financial institution, where customers can store valuable items such as documents, jewelry, or other personal possessions. These lockers are designed to offer a high level of security to protect against theft, fire, or other risks.

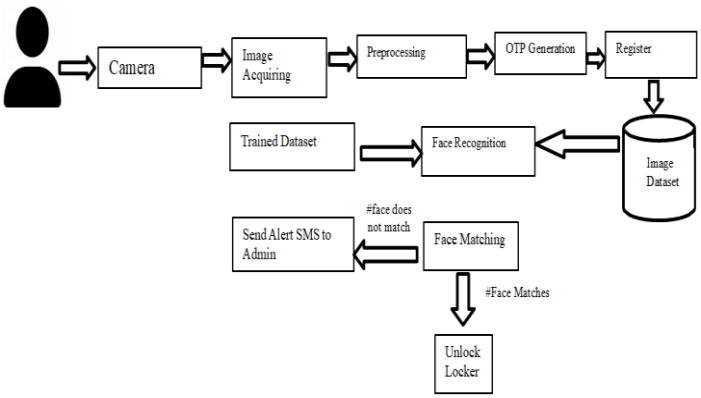

Fig -3 Data Flow Diagram

3. Result

The system was evaluated under different conditions, including variations in lighting facial expressions, and the presence of accessories. The following key findings were observed:

Face Detection accuracy: The system achieved an accuracy

Of 95% under controlled lighting conditions and 85% under real-world conditions, such as dim lighting or facial Obstructions.

OTP Verification Time: OTPs were successfully delivered Within 5 seconds on average, with a validation success rate of 99%.

The combination of face detection with OTP provided A significant improvement insecurity compared to traditional methods, as the dual authentication layers Reduced the likelihood of unauthorized access.

3. CONCLUSIONS

In conclusion the Bank Locker Security System using Machine Learning with Face detection and OTP authentication is a reliable and efficient solution for enhancing the security of bank lockers. The system uses facial recognition technology to accurately identify users and ensure that they are physically present, reducing the chances of unauthorized access. The integration of AI-based face recognition and OTP verification provides a robust, user-friendly and secure bank locker security system. It sets a new standard for protecting sensitive assets, offering a scalable solution that could be implemented in banks and financial institutions worldwide, ensuring both convenience and security in locker management.

ACKNOWLEDGEMENT

We would like to express our sincere gratitude to our advisor, Prof.I.Y.Inamdar, for their invaluable guidance, insightful comments, and continuous support throughout this research. We also thank [SMSMPITR,Akluj] for providing the necessary resources and funding for this project under the grant [Bank Locker Security System Using Machine Learning].

REFERENCES

[1] R. Usain, H. Jain, dan S. Pratap, “Enhancing bank security system using Face Recognition, Iris Scanner and Palm Vein Technology,” 2018 3rd International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Bimetal, pp. 1-5, 2018.

[2] M. I. G. P. S. Wijaya, A. Y. Hosoda, and I. W. A. Ari Mbawa, “Real time face recognition based on face descriptor and its application,” Telkom Nika, vol. 16, no. 2, pp. 739–746, April 2018.

[3] Face Liveness Detection with Recaptured Feature Extraction 2017 International Conference on Security, Pattern Analysis, and Cybernetics (SPAC) 978-1-5386-3016-7/17C 2017 IEEE.

[4] X. Liu, R. Lu and W. Liu, "Face liveness detection based on enhanced local binary patterns," 2017 Chinese Automation Congress (CAC), Jinan, 2017, pp. 6301-6305.

[5] K. Patel, H. Han, and A. K. Jain, “Secure Face Unlock: Spoof Detection on Smart phones,” IEEE Trans. Inf.

[6] Forensics Secure., vol. 11, no. 10, pp. 2268–2283, 2016..

[7] Di Wen, Hu Han, and A. K. Jain, “Face Spoof Detection with Image Distortion Analysis,” IEEE Trans. Inf. Forensics Secure., vol. 10, no. 4, pp. 746–761, 2015.

[8] S. Turnagain, N. Pooh, D. Windridge, A. Oorlam, N. Suki, and A. T. S. Ho, “Detection of face spoofing using visual dynamics,” IEEE Trans. Inf. Forensics Secure., vol. 10, no. 4, pp. 762– 777, 2015.

[9] G.-B. Huang, Z. Bai, L. L. C. Kasun, and C. M. Voong, “Local Receptive Fields Based Extreme Learning Machine,” IEEE Compute. Intel. Mag., vol. 10, no. 2, pp. 18–29,2015.

[10] Nallapa Reddy, Anusha & Sai, A & Srikar, B. (2022). Locker Security System Using Facial Recognition and One Time Password (OTP).

[11] Amit Verma, “A Multi Layer Bank Security System,” International Conference on Green Computing, Communication and Conservation of Energy (ICGCE), 2013.

[12] A Multi Layer Bank Security System by Amit Verma, published in 2013's International Conference on Green Computing, Communication, and Energy Conservation (ICGCE).

[13] K. D. Kulat, A. G. Keskar, and V. R. Satpute. "A novel methodology based on 2D—DWT and variance method for people detection and tracking in video surveillance applications" IEEE, 2014. 9th International Conference on Industrial and Information Systems (ICIIS).

[14] R. Gusain, H. Jain and S. Pratap, "Enhancing bank security system using Face Recognition, Iris Scanner and Palm Vein Technology," 2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU), Bhimtal, India, 2018, pp. 1-5, doi: 10.1109/IoT-SIU.2018.8519850.