ISSN: 3107-6513

Bank Vault Guardian Using Machine Learning Algorithms

Sushmitha. ES
Junior Researcher,
Department of Information Technology,
Sri Krishna Adithya College of Arts and Science,
Coimbatore, Tamil Nadu, India
23bsit260sushmithaes@skacas.ac.in

Mr. I. Gobi
Assistant Professor,
Department of Information Technology,
Sri Krishna Adithya College of Arts and Science,
Coimbatore, Tamil Nadu, India
gobii@skacas.ac.in

ABSTRACT:
Bank vault Guardian is very important in maintaining valuable assets of financial institutions. The conventional security system primarily depends on manual surveillance and relies on some predefined rules, which may not hold good against advanced threats. To overcome these limitations, this work proposes a bank vault guardian using machine learning algorithms. These systems study the surveillance data, records of access, and sensor inputs in order to learn the normal patterns of behavior. Ml algorithms find out unusual and suspicious activities. Unauthorized attempts to access the vault are detected in real-time with least human interference. In cases of security breaches, the system generates instant alerts. This intelligent approach limits fake alarms and quickens the response time. The model proposed will assure continuous monitoring of the bank vault. Altogether, this is a reliable and efficient solution to enhanced vault security.

KEYWORDS: *Bank Vault Security, Machine Detection, Intelligent Surveillance, Access Control Learning, Facial Recognition, Anomaly*

INTRODUCTION

Bank vault security is one of the most essential features of contemporary banking technology due to the growing number of bank vault security threats. Bank vaults that use security features such as locks and access cards offer basic safety from common threats but may not be effective against smart attacks. Manual verification is often required while entering the vaults that use locks and access cards. This may result in delays and mistakes.

To improve security, multi-factor authentications like One Time Password (OTP) have significantly gained acceptance in banking apps. OTP authentication ensures a second level of security with a time-dependent password that is randomly generated each time a person tries to access, making it difficult for unauthorized access. With machine learning algorithms, OTP authentication becomes more secure and trustworthy.

This proposal presents the development of a Bank Vault Guardian system that employs the use of machine learning algorithms in combination with OTP authentication. The machine learning solution carries out the evaluation of access patterns and system logs in a bid to detect any irregularities. Only those with authorized access, after the completion of OTP validation, are accorded entry into the vault. The innovation will enhance

ISSN: 3107-6513

precision, diminish cases of security threats, and provide real-time security surveillance

PROBLEM STATEMENT

Bank vaults keep very important assets and, thus, demand robust and reliable security systems. Most of the existing mechanisms for vault security depend basically on physical locks, access cards, passwords, and surveillance by people. These conventional systems are prone to security breaches, stolen credentials, insider threats, and other forms of human errors

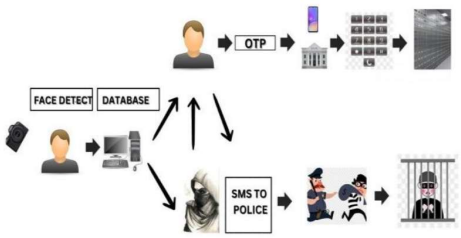
OBJECTIVE

The main objective of this is to design a secure bank vault guardian system using machine learning algorithms. The system aims to integrate OTP-based authentication to enhance access security.

SCOPE

The scope is to includes the development of an intelligent security framework for bank vault protection. It covers OTP-based user authentication and machine learning–based anomaly detection. The system is designed for real-time monitoring of vault access activities. It can be extended to integrate biometric authentication and advanced surveillance systems. The solution is scalable and suitable for modern banking security infrastructures.

System Architecture



User: Users are registered and valid credentials and identity information are provided.

Face Detection: The face detection module applies the use of machine learning to detect and authenticate the face features of the user.

OTP authentication module: A second layer of security is ensured by the use of a time-sensitive password provided by the OTP authentication module

Lock Access Module: The locker access module enables entry only after completing all steps in a successful authentication process.

Machine learning algorithms analyze locker-access behaviors prior to authorizing access. On successful verification, a secure locker mechanism unlocks. Unauthenticated attempts result in denial and raise an alarm.**FACE RECOGNITION ALGORITHM**

Face Recognition Algorithm

Face recognition is a method of biometric identification that can verify or authenticate a person based on their facial information. It takes a snapshot from a camera and processes the image to locate the face. Artificial intelligence algorithms pick distinct facial details and then match them with the templates stored in the data bank. Depending on the result, the system unlocks access for the user or not.

Algorithm Steps

Record the actual image of the user from a camera.

Convert the image into grayscale and resize the image using the following commands.

Detect face region by using Haar Cascade algorithm.

Extract the facial features by utilizing the Local Binary Pattern Histogram (LBPH) technique.

Compare the extracted features to the existing facial dataset.

Find a similarity measurement for the input face and images in the database**.**

Access if the similarity score is within the threshold; otherwise, deny.

Flowchart Explanation

The procedure for face recognition includes image acquisition from the camera. Then, image preprocessing takes place to improve image clarity. Face detection follows next to detect the region of

ISSN: 3107-6513

interest. Feature extraction is used to get the distinctive patterns from the face. Then, the features are matched to the database. Finally, the result is used to make a decision to accept or reject the user.

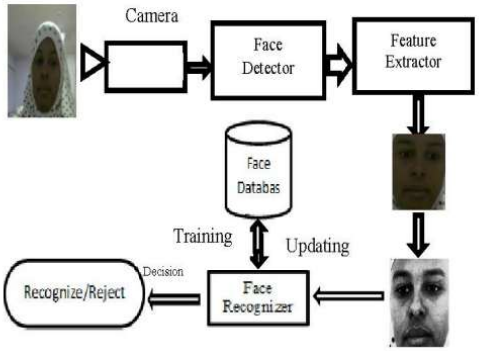
Specifically Used Algorithms

Haar Cascade Algorithm:

The Haar Cascade is applied in face detection in a fast and efficient manner using a face detection program. It detects regions of interest by analyzing contrast in images. It is preferred in real-time applications since it is less computationally expensive**.**

Local Binary Pattern Histogram (LBPH):
The LBPH is employed for the extraction and recognition of facial features. It transforms the textures of the facial features into binary features and then forms histograms for matching purposes. LBPH withstands varying lighting conditions and performs very well in real-time systems.

Convolutional Neural Network (CNN):
CNN is a deep learning approach for face recognition tasks. It enables automatic learning of complex facial features from large amount of data. CNN offers greater accuracy but is computationally intensive compared to traditional approaches**.**



BANK LOCKER

The vault guardian system theoretical foundations of this system include access control, authentication, and anomaly detection, all of these improved through ML. In standard bank locker systems, for instance, security relies on mechanical keys or PIN codes, factors that can be copied or brute-forced for attack. With ML algorithms inserted into it, this system transforms into an intelligent guardian**.**

AUTHENTICATION
Biometric Recognition: Fingerprints, facial characteristics, and iris scans are taken and searched for a match among preexisting templates.

Role of Machine Learning: The use of Support Vector Machines (SVM) and Convolutional Neural Networks (CNN), for example, increases the accuracy of recognition through the learned unique patterns of the biometric inputs.

Theoretical Foundation: Pattern recognition results in only valid individuals being granted access while minimizing the probability of false rejection.

ACCESS CONTROL

Digital Locking Mechanism: The electronic lock operates through a secured circuit**.**

ML Integration: Predictive models detect anomalies based on attempts to gain access by analyzing user behaviors**.**

Underlying Theory: Decision-making models or the classification algorithms calculate the confidence levels for the grant or denial of access.

Surveillance & Anomaly Detection

ISSN: **3107-6513**

Sensor Data: These generate data from the sensors and CCTV cameras**.**
ML Application: Unsupervised machine learning points towards unusual patterns of locker usage behavior**.**
Anomaly detection theory: Anomalies or unusual events can be abstracted from data mathematically, making it possible to react before they occur.

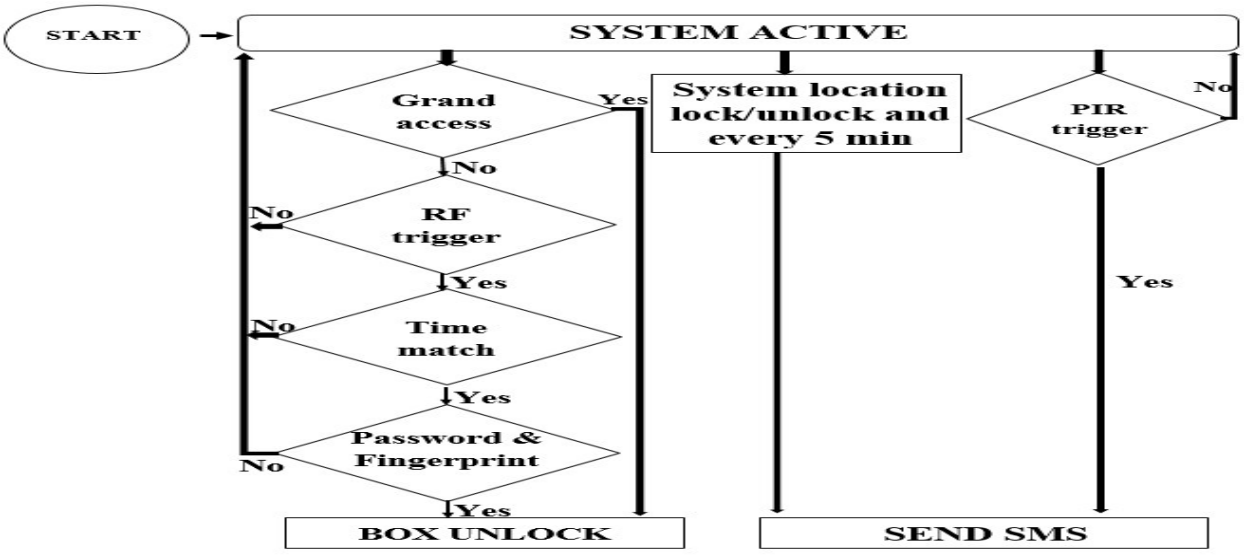
Audit & Logging

Data Gathering: Each attempted access is recorded along with time, identity, and locker number.

ML Analysis: Past records of use are analyzed using predictive analytics techniques to predict possible misuse.

Integration in Guardian Framework

The Bank Locker Module is the granular security layer in the overall vault guardian system. While the vault guardian is responsible for securing the entire vault environment, the bank locker module is responsible for securing individual lockers.



OTP AUTHENTICATION

One-Time Password (OTP) authentication is a critical security mechanism employed in the *Bank Vault Guardian* system to ensure robust access control and prevent unauthorized entry. OTP authentication enhances traditional security methods by generating a unique, time-sensitive password for each authentication attempt, thereby significantly reducing the risk of password theft, replay attacks, and brute-force intrusions.

The proposed system, OTP authentication acts as a **second layer of verification** alongside machine learning–based anomaly detection. When a user attempts to access the bank vault system, an OTP is dynamically generated and securely delivered to the registered user through a trusted communication channel such as SMS or email. The OTP remains valid only for a short duration, ensuring that even if intercepted, it cannot be reused.

The integration of OTP authentication with machine learning algorithms strengthens the system by combining **user verification** with **behavioral analysis**. While the OTP confirms

the legitimacy of the user, the machine learning model analyzes access patterns, login
time, location, and historical behavior to detect suspicious activities. If abnormal patterns are identified, additional authentication or access denial is triggered.

Overall, OTP authentication plays a vital role in enhancing the reliability, confidentiality, and integrity of the *Bank Vault Guardian* system. By incorporating OTP with machine learning techniques, the proposed solution delivers a highly secure, intelligent, and adaptive vault protection

ISSN: 3107-6513

framework suitable for modern banking environments.

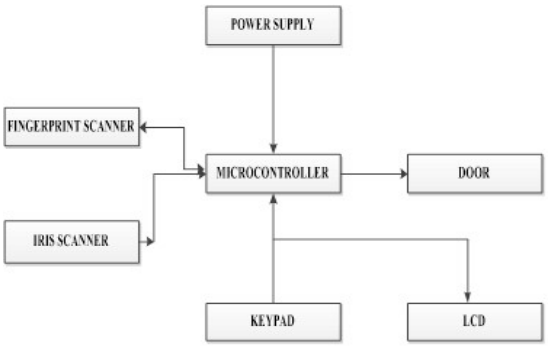
Proposed System (Theory)

The proposed system, titled **Bank Vault Guardian Using Machine Learning Algorithm**, is designed to provide a highly secure, intelligent, and automated protection mechanism for bank vaults. The system overcomes the limitations of traditional security approaches by integrating **machine learning–based behavior analysis** with **OTP-based multi-factor authentication**, ensuring enhanced accuracy and reliability in access control. In this system, authorized users are registered with unique credentials and historical access data such as login time, access frequency, and location. A machine learning algorithm is trained on this historical data to learn normal access patterns. During each access attempt, the trained model evaluates real-time user behavior and determines whether the request aligns with authorized usage patterns or represents a potential threat.

Upon successful behavioral verification, an **OTP (One-Time Password)** is generated and sent to the registered user through a secure communication channel. The OTP is time-bound and valid for a single session, ensuring protection against replay attacks and unauthorized reuse. Access to the vault is granted only when both machine learning validation and OTP authentication are successfully completed.

If abnormal behavior or suspicious activity is detected, the system automatically triggers security alerts, denies access, and logs the incident for further analysis. This adaptive mechanism allows the system to continuously improve its detection accuracy over time.

Overall, the proposed system enhances bank vault security by combining **intelligent decision-making**, **real-time monitoring**, and **multi-layer authentication**, making it suitable for modern banking environments where high security and reliability are critical.



METHODOLOGY

The methodology of the proposed **Bank Vault Guardian Using Machine Learning Algorithm** focuses on implementing a secure, intelligent, and adaptive bank locker protection system by integrating machine learning techniques with OTP-based authentication. The system operates through a sequence of well-defined stages to ensure accurate user verification and effective threat detection.

1. Data Collection

Historical bank locker access data is collected from authorized users. This data includes parameters such as user identification, access time, frequency of access, location, and previous authentication records. The collected dataset forms the foundation for training the machine learning model.

2. Data Preprocessing

The collected data is cleaned and preprocessed to remove inconsistencies, missing values, and noise. Relevant features are extracted and normalized to improve model performance and ensure accurate behavioral pattern recognition.

3. Machine Learning Model Training

A machine learning algorithm is trained using the preprocessed historical data to learn normal access behavior patterns of users. Algorithms such as Decision Tree, Random Forest, or Support Vector Machine can be employed to classify access attempts as normal or suspicious.

4. Real-Time Behavior Analysis

During each locker access request, the trained machine learning model evaluates real-time user behavior and compares it with learned patterns. If the behavior deviates from normal patterns, the system identifies it as suspicious and initiates security actions.

5. OTP Generation and Verification

For verified access attempts, a One-Time Password (OTP) is dynamically generated and sent to the

ISSN: 3107-6513

registered mobile number or email of the user. The OTP is time-bound and valid for a single session. Access is granted only upon successful OTP verification.

6. Access Control and Locker Operation

Once both machine learning validation and OTP authentication are successful, the system unlocks the bank locker. All access activities are securely logged for auditing and future reference.

7. Alert and Logging Mechanism

If suspicious behavior or invalid OTP attempts are detected, the system denies access, triggers alerts to bank authorities, and records the incident. This enhances accountability and improves system security.

Advantages of the Methodology

- Multi-layer security approach
- Intelligent threat detection
- Reduced unauthorized access
- Adaptive and scalable system

CONCLUSION

The **Bank Vault Guardian Using Machine Learning Algorithm** project successfully presents a secure and intelligent approach to bank locker protection by integrating machine learning–based behavior analysis with OTP authentication. The proposed system addresses the limitations of traditional locker security mechanisms by introducing adaptive decision-making and multi-layer authentication.

Overall, the proposed Bank Vault Guardian system offers a reliable, scalable, and future-ready solution for modern banking environments. With further enhancements such as biometric authentication and advanced deep learning models, the system can be extended to achieve even higher levels of security and automation.

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to all those who have contributed to the successful completion of this project titled **"Bank Vault Guardian Using Machine Learning Algorithm."**

I extend my heartfelt thanks to my project guide for their valuable guidance, constant encouragement, and insightful suggestions throughout the course of this project. Their expertise and support played a crucial role in shaping the project.

I am grateful to the Head of the Department and all faculty members for providing the necessary resources, technical knowledge, and academic support required for the completion of this work.

I also thank my institution for providing the infrastructure and facilities that enabled smooth execution of the project. My sincere appreciation goes to my friends and classmates for their cooperation, discussions, and assistance during the development of this project.

Finally, I would like to express my deepest gratitude to my family for their continuous support, motivation, and encouragement, which inspired me to complete this project successfully.

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 (IoTSIU), 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

ISSN: **3107-6513**

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.