AI Powered Bank Locker Security System

[1]Dr. T. Srinivasulu,[2]L. Susmitha,[3] S. Divya Sri,[4]P. Swarna Latha

[1]Principal, Princeton Institute of Engineering & Technology For Women

[2,3,4]B. Tech Students, Department of Electronics And Communication Engineering, Princeton Institute of Engineering & Technology For Women

ABSTRACT

The rapid advancement of artificial intelligence has enabled the development of smarter and more secure security systems for financial institutions. Traditional bank locker security mechanisms mainly rely on physical keys, passwords, or manual surveillance, which are vulnerable to theft, unauthorized access, and human error. To address these limitations, the proposed AI Powered Bank Locker Security System integrates artificial intelligence with modern authentication and monitoring technologies to enhance the safety of bank lockers. The system utilizes AI-based facial recognition, biometric authentication, and intelligent monitoring to ensure that only authorized users can access the locker. Machine learning algorithms analyze facial features and user data to verify identity with high accuracy, while real-time monitoring helps detect suspicious activities around the locker area. In addition, the system can send instant alerts and notifications to bank authorities in case of unauthorized access attempts or abnormal behavior. Furthermore, the proposed system improves security by maintaining digital logs of locker access, enabling efficient tracking and auditing. AI-based analytics can also detect unusual patterns and potential security threats, thereby preventing fraud and ensuring enhanced protection of valuable assets stored in bank lockers. By combining artificial intelligence, biometrics, and automated monitoring, the system offers a reliable, efficient, and advanced security solution for modern banking infrastructure. Overall, the AI Powered Bank Locker Security System aims to reduce security risks, eliminate dependency on traditional keys, and provide a smart, automated, and highly secure locker management system for banks.

Keywords: Artificial Intelligence, Bank Locker Security, Facial Recognition, Biometric Authentication, Machine Learning, Smart Surveillance, Access Control System, Fraud Detection, Secure Banking, Real-Time Monitoring.

I. INTRODUCTION

In the modern banking environment, ensuring the safety and security of customer assets is a critical responsibility. Bank lockers are widely used by customers to store valuable items such as jewelry, documents, and other important possessions. Traditional bank locker systems generally rely on mechanical keys, password-based systems, and manual verification by bank staff. Although these methods have been used for many years, they have several limitations, including the risk of key duplication, unauthorized access, and human errors during verification. As technology advances and security threats increase, there is a growing need for more intelligent and automated security systems in banking infrastructure.

Artificial Intelligence (AI) has emerged as a powerful technology capable of enhancing security systems through intelligent decision-making and automated monitoring. AI-based security solutions can analyze large amounts of data, identify patterns, and detect suspicious activities more efficiently than traditional methods. In the context of bank locker systems, AI can be integrated with biometric authentication techniques such as facial recognition, fingerprint scanning, and behavioral analysis to ensure that only authorized individuals are granted access to the locker. This significantly reduces the chances of unauthorized entry and improves overall system reliability.

An AI Powered Bank Locker Security System provides a smart and automated approach to locker access control and monitoring. The system verifies

the identity of users using advanced AI algorithms and biometric authentication, ensuring that access is granted only after successful verification. Additionally, intelligent surveillance systems can continuously monitor locker areas and detect abnormal activities in real time. In case of suspicious attempts, the system can generate alerts and notify bank authorities immediately, enabling quick response to potential security threats.

Furthermore, the integration of AI technology enables the system to maintain secure digital records of locker usage, including access time, user identity, and activity logs. These records help banks maintain transparency, improve auditing processes, and strengthen overall security management. By replacing traditional security mechanisms with AI-driven technologies, banks can provide a safer and more efficient locker service to their customers.

Therefore, the proposed AI Powered Bank Locker Security System aims to enhance locker security by combining artificial intelligence, biometric authentication, and intelligent monitoring. This approach not only improves protection against theft and unauthorized access but also supports the development of smarter and more secure banking systems in the future.

II. LITERATURE SURVEY

1. Title: AI Based Smart Security System Using Face Recognition

Author: A. Kumar, R. Singh

Abstract:
This research presents an intelligent security system that uses artificial intelligence and facial recognition technology to control access to secure environments. The system captures the user's facial image through a camera and processes it using machine learning algorithms to verify identity. If the detected face matches the authorized database, access is granted; otherwise, the system triggers an alert. The study demonstrates that AI-based facial recognition significantly improves authentication accuracy and reduces unauthorized access compared to traditional security systems.

2. Title: Biometric Authentication for Secure Banking Systems

Author: S. Patel, M. Shah

Abstract:
This study explores the use of biometric technologies such as fingerprint recognition and facial authentication in banking security systems. The authors discuss how biometric authentication enhances the security of banking services by providing unique identity verification. The system integrates biometric sensors with digital verification methods to prevent identity theft and fraud. Experimental results show that biometric-based security systems provide higher reliability and better protection than password-based authentication mechanisms.

3. Title: Smart Locker Security System Using Internet of Things (IoT)

Author: R. Gupta, P. Sharma

Abstract:
This paper proposes an IoT-based smart locker security system designed to improve locker safety and monitoring. The system uses sensors, cameras, and microcontrollers to monitor locker access and send real-time notifications to administrators. The integration of IoT devices enables remote monitoring and automated alert generation during unauthorized access attempts. The results show that IoT-enabled locker systems can significantly improve security management and reduce manual supervision.

4. Title: Machine Learning Based Intrusion Detection System

Author: J. Brown, K. Williams

Abstract:
The authors present a machine learning-based intrusion detection system capable of identifying suspicious activities in secure environments. The system analyzes behavioral patterns and network data to detect anomalies and possible security threats. By applying classification algorithms, the system can differentiate between normal and abnormal behavior with high accuracy. This approach demonstrates how machine learning techniques can enhance modern security systems by enabling proactive threat detection.

5. Title: Intelligent Surveillance System Using Deep Learning

Author: L. Chen, Y. Zhang

Abstract:
This research focuses on developing an intelligent surveillance system using deep learning techniques for automated monitoring and security enhancement. The system uses deep neural networks to detect human presence, identify individuals, and recognize suspicious activities in real time. The proposed surveillance framework improves accuracy in monitoring restricted areas and assists security personnel in preventing security breaches. The study highlights the effectiveness of deep learning in strengthening surveillance and access control systems.

III. EXISTING SYSTEM

The existing bank locker security systems are primarily based on traditional mechanical and manual security mechanisms. In most banks, locker access is controlled through a dual-key system where one key is held by the customer and the other by the bank authority. Both keys must be used together to open the locker. While this method has been widely used for many years, it depends heavily on physical keys and manual verification processes, which may create security vulnerabilities. Loss or duplication of keys can lead to unauthorized access, posing a risk to the valuables stored in the lockers.

In addition to key-based access, banks often rely on manual identity verification performed by bank staff before allowing customers to access their lockers. This process may involve checking identity documents or verifying signatures. However, manual verification is time-consuming and may lead to human errors. In busy banking environments, staff may not always thoroughly verify every user, which increases the chances of security breaches or fraudulent access.

Many traditional locker systems also lack intelligent monitoring and real-time alert mechanisms. Surveillance cameras may be installed in locker rooms, but they generally function only as recording devices rather than proactive security tools. These systems do not automatically detect suspicious activities or unauthorized access attempts. As a result, security threats may only be identified after an incident has occurred, making it difficult to prevent theft or misuse.

Furthermore, the existing systems do not maintain advanced digital records or analytical insights about locker usage. Access logs are often recorded manually or stored in simple databases without advanced monitoring or analysis capabilities. This limitation makes it difficult for banks to track unusual patterns or identify potential threats in advance. Therefore, traditional locker security systems are limited in their ability to provide intelligent, automated, and highly secure protection for valuable assets.

IV. PROPOSED SYSTEM

The proposed AI Powered Bank Locker Security System introduces an intelligent and automated approach to enhance the security of bank lockers by integrating artificial intelligence, biometric authentication, and smart monitoring technologies. Unlike traditional locker systems that rely on physical keys and manual verification, the proposed system uses AI-based facial recognition and biometric verification methods to ensure that only authorized users can access the lockers. This

significantly improves the level of security and minimizes the risk of unauthorized access.

In the proposed system, the user's identity is verified using advanced biometric technologies such as facial recognition or fingerprint authentication. When a user attempts to access a locker, the system captures the user's biometric data through cameras or sensors and compares it with the stored database using machine learning algorithms. If the authentication is successful, the system allows access to the locker; otherwise, it denies access and immediately generates an alert to the bank authorities. This automated verification process reduces human intervention and increases the accuracy of identity validation.

The system also incorporates intelligent surveillance and monitoring features. AI-enabled cameras continuously monitor the locker area and analyze activities in real time. If any suspicious behavior or unauthorized attempt is detected, the system automatically sends alerts or notifications to security personnel. This real-time monitoring helps in preventing security breaches and allows quick response to potential threats.

Additionally, the proposed system maintains secure digital records of locker usage, including user identity, access time, and activity logs. These records can be analyzed using AI algorithms to detect unusual patterns or repeated unauthorized access attempts. Such analytics help banks strengthen their security management and improve auditing processes.

Overall, the AI Powered Bank Locker Security System provides a smart, reliable, and efficient solution for modern banking security. By integrating artificial intelligence, biometric authentication, and automated monitoring, the proposed system enhances locker protection, reduces security risks, and ensures better safety for customers' valuable assets.

V. BLOCK DIAGRAM

The AI Powered Bank Locker Security System is designed with multiple integrated components that work together to provide secure, intelligent, and automated locker access control. The system architecture mainly consists of input modules, processing modules, authentication mechanisms, monitoring units, and a central database. These components interact with each other to verify user identity, control locker access, and monitor activities in real time.

The architecture begins with the user authentication module, where the customer initiates the locker access request. In this stage, biometric devices such as a facial recognition camera or fingerprint scanner capture the user's biometric data. The captured data is sent to the processing unit where artificial intelligence algorithms analyze the input and compare it with the stored user information in the database. This verification process ensures that only registered and authorized users can proceed to access the locker.

After the biometric data is captured, the AI processing module performs feature extraction and identity verification using machine learning models. The system checks whether the biometric data matches the authorized records stored in the database. If the match is successful, the system sends a command to the locker control unit to unlock the locker electronically. If the verification fails, the system denies access and triggers a security alert.

The locker control module manages the physical locking and unlocking mechanism of the locker. This module is connected to electronic locks that operate based on authentication results. When the system receives a valid authentication signal, the locker opens for the authorized user. At the same time, the system records the access information such as user identity, time of access, and locker number in the system database for future reference.

Another important component of the architecture is the monitoring and alert system. AI-powered surveillance cameras continuously monitor the locker area to detect suspicious activities or unauthorized attempts. If any abnormal behavior is identified, the system generates alerts and notifies bank authorities

immediately. This ensures quick response and enhances the overall security of the locker environment.

Finally, the database and management module stores user biometric data, locker details, access logs, and security records. Bank administrators can access this information through a management interface to monitor locker usage, review activity logs, and maintain system security. The integration of these modules creates a robust architecture that improves security, automation, and efficiency in bank locker management.

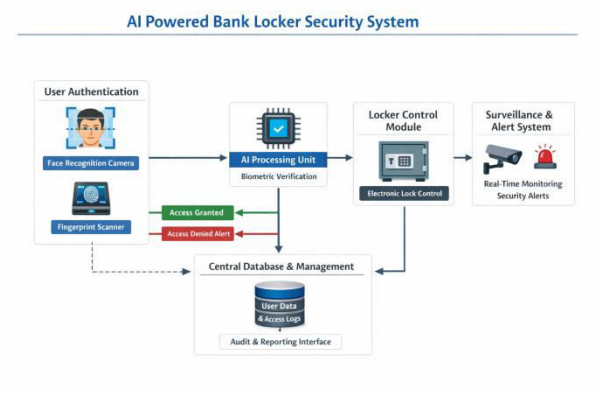

Fig 5.1: Block Diagram

VI. IMPLEMENTATION

Fig 6.1: Secure Locker Area

Fig 6.2: Multi-Screen Surveillance and Access Monitoring Dashboard

Fig 6.3: AI Facial Recognition Authentication for Bank Locker Access

Fig 6.4: AI Locker Security System – Administrative Dashboard and Access Log Monitoring

VII. CONCLUSION

The AI Powered Bank Locker Security System provides an advanced and intelligent solution to enhance the safety of bank lockers. Traditional locker systems mainly rely on mechanical keys and manual verification, which can lead to security vulnerabilities such as key duplication, human errors, and unauthorized access. By integrating artificial intelligence and biometric authentication technologies, the proposed system significantly improves the level of security and reliability in locker management.

The system utilizes AI-based facial recognition, biometric verification, and real-time monitoring to ensure that only authorized users can access the lockers. Automated identity verification reduces the dependency on manual processes and minimizes the chances of fraudulent access. In addition, intelligent surveillance and alert mechanisms help detect suspicious activities instantly, enabling quick response from bank authorities and preventing potential security breaches.

Furthermore, the system maintains digital access logs and monitoring records, which allow banks to track locker usage and analyze security patterns efficiently. This feature improves transparency, accountability, and auditing processes within banking institutions. The integration of AI technology not only enhances security but also increases operational efficiency and user convenience.

Overall, the proposed AI Powered Bank Locker Security System offers a secure, reliable, and smart solution for modern banking infrastructure. By combining artificial intelligence, biometric authentication, and automated monitoring, the system ensures enhanced protection of valuable assets while supporting the development of smarter and more secure banking services in the future.

VIII. FUTURE SCOPE

The AI Powered Bank Locker Security System can be further enhanced by integrating more advanced technologies to improve security, efficiency, and user convenience. In the future, the system can incorporate multiple biometric authentication methods such as iris recognition, palm vein scanning, and voice recognition to provide multi-layer security. Using multiple authentication factors will further reduce the possibility of unauthorized access and strengthen the overall protection of bank lockers.

Another potential improvement is the integration of Internet of Things (IoT) technology to enable smarter monitoring and remote management of locker systems. IoT sensors can detect unusual activities such as forced locker openings, tampering attempts, or environmental changes like temperature and humidity inside locker rooms. These sensors can automatically send real-time alerts to bank authorities through mobile applications or centralized monitoring systems, allowing faster response to security threats.

The system can also be enhanced by implementing blockchain technology to maintain secure and tamper-proof access records. Blockchain can store locker access logs in a decentralized and highly secure manner, ensuring that the records cannot be modified or deleted. This would increase transparency and trust in the system while improving auditing and compliance processes for financial institutions.

Additionally, future developments may include mobile application integration, allowing customers to schedule locker access, receive real-time notifications, and verify their identity through secure mobile authentication. Artificial intelligence can also be used for predictive analytics to identify unusual access patterns and detect potential security threats before they occur. These enhancements will make the system more intelligent, user-friendly, and highly secure, supporting the evolution of modern digital banking infrastructure.

IX. REFERENCES

[1] A. B. Gadewar, Y. D. Satre, S. Y. Girme, and S. Walunj, “Implementation of Bank Locker Authentication System Using Facial Recognition,” *International Journal of Scientific Research in Science, Engineering and Technology*, 2023.
DOI: https://doi.org/10.32628/IJSRSET23103101

[2] Y. Kumar and V. Dogra, "Bank Locker Security System Using Machine Learning," *International Research Journal of Engineering and Technology*, vol. 11, no. 12, 2024.
DOI: https://doi.org/10.13140/RG.2.2.31215.92323
[3] P. Kandekar, A. Pisare, and R. Margale, "Bank Locker Security System Using Machine Learning with Face and Liveness Detection," *International Journal of Scientific Research in Science, Engineering and Technology*, 2022.
DOI: https://doi.org/10.32628/IJSRSET2293255
[4] M. Krishnaveni and M. Myilavahanan, "IoT Based Bank Locker Security System with Face Recognition," *Grenze International Journal of Engineering and Technology*, 2023.
DOI: https://doi.org/10.13140/RG.2.2.25660.36480
[5] S. Kale, A. Nair, and M. Pagar, "Bank Locker Security System Using Machine Learning with Face Detection and OTP Authentication," *IRJET*, 2024.
DOI: https://doi.org/10.13140/RG.2.2.23892.71043
[6] U. Navalgund and K. Priyadharshini, "Crime Intention Detection System Using Deep Learning," *IEEE Conference on Computational Intelligence*, 2018.
DOI: https://doi.org/10.1109/CAC.2017.8243391
[7] T. Nguyen, B. Lakshmanan, and W. Sheng, "A Smart Security System with Face Recognition," *arXiv*, 2018.
DOI: https://doi.org/10.48550/arXiv.1812.09127
[8] D. N. Parmar and B. B. Mehta, "Face Recognition Methods and Applications," *International Journal of Computer Applications*, 2014.
DOI: https://doi.org/10.48550/arXiv.1403.0485
[9] B. Mugalu, R. Wamala, J. Serugunda, and A. Katumba, "Face Recognition as a Method of Authentication in a Web-Based System," *arXiv*, 2021.
DOI: https://doi.org/10.48550/arXiv.2103.15144
[10] E. Zhou, Z. Cao, and Q. Yin, "Naive-Deep Face Recognition: Touching the Limit of LFW Benchmark or Not?" *arXiv*, 2015.
DOI: https://doi.org/10.48550/arXiv.1501.04690
[11] R. Gusain, H. Jain, and S. Pratap, "Enhancing Bank Security System Using Face Recognition, Iris Scanner and Palm Vein Technology," *IEEE International Conference on Internet of Things: Smart Innovation and Usages*, 2018.
DOI: https://doi.org/10.1109/IoT-SIU.2018.8519881
[12] Y. Wang, T. Bao, C. Ding, and M. Zhu, "Face Recognition in Real-World Surveillance Videos with Deep Learning," *IEEE Conference on Computer Vision*, 2017.
DOI: https://doi.org/10.1109/ICCV.2017.123
[13] L. Pang, "Research on Privacy Security of Face Recognition Technology," *Sensors*, vol. 22, 2022.
DOI: https://doi.org/10.3390/s22030910
[14] K. Patel, H. Han, and A. Jain, "Secure Face Unlock: Spoof Detection on Smartphones," *IEEE Transactions on Information Forensics and Security*, 2016.
DOI: https://doi.org/10.1109/TIFS.2016.2578282
[15] M. Simmler and L. Frischknecht, "Facial Recognition Technology in Law Enforcement," *Computer Law & Security Review*, 2024.
DOI: https://doi.org/10.1016/j.clsr.2024.105735