ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940

www.ijsem.org

Vol 18, Issue.2 April 2024

BANK LOCKER SECURITY SYSTEM

1.DR SUDHAKAR, 2. G. VANAJAKSHI, 3. G. JAHNAVI, 4.G. NAGAVASAVI

1.ASSOSCAITE PROFESSOR,2,3&4.UG SCHOLAR

DEPARTMENT OF ECE, MALLA REDDY ENGINEERING COLLEGE FOR WOMEN, HYDERABAD

ABSTRACT

This paper will focused on effective recognizing and controlling system for Bank locker room which is fully self-determining. In cases of robberies, it's commonly happen that the banned entrance in the locker room area which can be detected by our security system. If the robbery take place the banks are not be capable to recognize the robber due to absence of the proof by using the current human operated security system. Development of various sensors has enabled systems to have preventive and corrective measures in this regard significantly. In order to deliver a concrete security solution for critically important and confidential documents and goods, we proposed an Automated Safety Vault with Double Layered Defense Mechanism. The solution comprised of an Electronic Lock driven by password verification and a Biometric authentication for users using a Fingerprint scanning and sensing tool. Both of these two layers ensured the authenticity of the user by preventing any unauthorized access to the Vault. The system was then implemented in a prototype scope for testing and validation of the proposals. The implemented system and testing data showed that the Automated Safety Vault with all its security features had successful operation. The specification of the whole system as well as the results is observed and verified.

INTRODUCTION

The introduction of a banking locker security system heralds a new era of confidence and reliability in safeguarding valuable assets within the banking sector. In today's world, where security concerns loom large, ensuring the protection of customers' valuables is paramount for financial institutions. The banking locker security system stands as a bulwark against threats such as theft, unauthorized access, and environmental damage, offering a comprehensive and robust solution to meet these challenges head-on. At the heart of the banking locker security system lies a sophisticated array of technological components and physical infrastructure designed to thwart potential security

breaches. Biometric authentication mechanisms, such as fingerprint or iris scanning, serve as the first line of defense, ensuring that only authorized individuals can access the lockers. This advanced authentication is complemented by secure access control systems, which employ smart cards, PIN codes, or encrypted keys unique to each customer, meticulously managing to regulate access permissions and maintain detailed audit logs.

Fig: Bank Locking security system

Furthermore, the physical security features of the locker facility are fortified to resist tampering and unauthorized entry. Reinforced doors, secure locks, and alarm systems form a formidable barrier against theft, while CCTV cameras and surveillance equipment monitor activities in real-time, enabling prompt responses to any suspicious behavior. Additionally, fire detection and suppression systems, along with environmental controls, mitigate the risk of damage to stored valuables, ensuring their preservation in adverse conditions. Beyond mere security measures, modern banking locker systems offer remote monitoring and management capabilities, empowering bank staff to oversee operations and respond swiftly to security incidents from a centralized location. This enhances operational efficiency and enables proactive intervention to safeguard assets and uphold the trust of customers. In essence, banking locker security systems represent the pinnacle of asset protection within the banking sector, offering unparalleled security, reliability, and peace of mind to customers. By leveraging advanced technology, stringent security protocols, and robust physical infrastructure, these systems not only mitigate the risk of loss but also reinforce customer confidence in the integrity and security of financial institutions.

LITERATURE SURVEY

The literature survey for the proposed banking locker security system encompasses an in-depth analysis of existing research, studies, and technologies related to security measures and asset protection within the banking sector. Numerous scholarly articles, industry reports, and academic studies have

explored various aspects of banking security, including physical security, biometric authentication, access control systems, surveillance technologies, regulatory compliance, operational efficiency, and customer satisfaction. Studies have highlighted the importance of implementing robust security measures to safeguard valuable assets stored within banking facilities, emphasizing the need for advanced technological solutions and stringent security protocols to mitigate security threats such as theft, unauthorized access, and environmental damage. Research has also underscored the significance of regulatory compliance in ensuring the protection of customer assets and maintaining the integrity of the banking system. Advancements in biometric authentication technology have been a focal point of research, with studies examining the effectiveness and reliability of biometric identifiers such as fingerprints, iris patterns, and facial recognition in enhancing security and preventing unauthorized access to banking lockers. Additionally, research has explored the integration of access control systems, surveillance equipment, and environmental controls to create a comprehensive security infrastructure that can withstand various security threats and environmental hazards. Operational efficiency has emerged as another key area of focus, with studies investigating the integration of remote monitoring and management capabilities to streamline administrative processes, enhance oversight, and improve response times to security incidents or emergencies. Furthermore, research has examined the role of customer confidence in driving satisfaction and loyalty within the banking sector, highlighting the importance of providing customers with a secure and reliable storage solution for their valuables. Cost-effectiveness has also been a consideration in the literature, with studies evaluating the total cost of ownership of security systems and identifying strategies for optimizing resource allocation while maintaining robust security measures. Finally, research has emphasized the importance of continuous improvement and innovation in banking security systems to address evolving security threats and technological advancements effectively. Overall, the literature survey provides valuable insights into the current state of banking security, highlighting key trends, challenges, and opportunities in the field. By synthesizing existing\ research and knowledge, the proposed banking locker security system can leverage best practices and innovative solutions to enhance

ISSN2454-9940

www.ijsem.org

Vol 18, Issue.2 April 2024

security, regulatory compliance, operational efficiency, customer satisfaction, and cost-effectiveness within the banking institution.

PROPOSED SYSTEM

The proposed system for the banking locker security system entails the integration of advance technology, robust physical infrastructure, and stringent security protocols to create a comprehensive solution for safeguarding valuable assets stored within banking facilities. Here's an outline of the proposed system components:

- Biometric Authentication: Implementing biometric authentication mechanisms such as fingerprint or iris scanning to ensure that only authorized individuals can access the banking lockers. Biometric identifiers will be securely stored and matched against the stored data to grant access.

- Secure Access Control: Utilizing smart cards, PIN codes, or encrypted keys unique to each customer to regulate access permissions. Access control systems will be managed centrally, with detailed audit logs maintained to track access activities.

- Surveillance Systems: Deploying CCTV cameras and surveillance equipment throughout the locker facility to monitor activities in real-time. Video feeds will be monitored by security personnel to detect and respond to any suspicious behavior promptly.

- Physical Security Features: Reinforcing the physical infrastructure of the locker facility with robust doors, secure locks, and alarm systems to deter theft and unauthorized entry. Environmental controls will also be implemented to mitigate risks related to temperature, humidity, and fire.

- Remote Monitoring and Management: Implementing remote monitoring and management capabilities to enable centralized oversight of locker facilities. Security personnel will have access to real-time monitoring tools and alerts to respond swiftly to security incidents or emergencies.

- Integration with Banking Systems: Integrating the locker security system with existing banking systems to streamline administrative processes and

ISSN2454-9940

www.ijsem.org

Vol 18, Issue.2 April 2024

enhance customer experience. This includes automating locker rental procedures, billing, and notifications to customers.

- Regular Maintenance and Upgrades: Establishing a schedule for regular maintenance and upgrades to ensure the continued effectiveness and reliability of the locker security system. This includes software updates, equipment inspections, and repairs as needed.
- Employee Training and Awareness: Providing comprehensive training to bank staff on the operation and management of the locker security system. Additionally, raising awareness among employees about security best practices and protocols to minimize the risk of internal security breaches.

Overall, the proposed system aims to provide a comprehensive and reliable solution for safeguarding valuable assets within banking facilities. By leveraging advanced technology, robust physical infrastructure, and stringent security protocols, the system ensures the safety, integrity, and confidentiality of stored assets, thereby enhancing customer trust and confidence in the banking institution.

IMPLEMENTATION

The methodology for implementing the proposed banking locker security system follows a systematic and comprehensive approach, commencing with a thorough needs assessment of the banking institution's security requirements. This involves considering various factors such as facility size, asset volume and value, regulatory compliance, and customer expectations. Subsequently, a comprehensive literature review explores existing research and technologies pertinent to banking security, encompassing physical security measures, biometric authentication, access control systems, surveillance technologies, regulatory compliance, operational efficiency, and customer satisfaction. The technology evaluation phase involves a careful examination of available security technologies, considering factors like effectiveness, reliability, scalability, compatibility, and cost-effectiveness. Collaboration with security experts, vendors, and industry peers assists in identifying the most suitable options. The system design is then tailored to the specific needs of the institution, encompassing

configurations for biometric authentication, access control, surveillance, physical security features, and environmental controls.

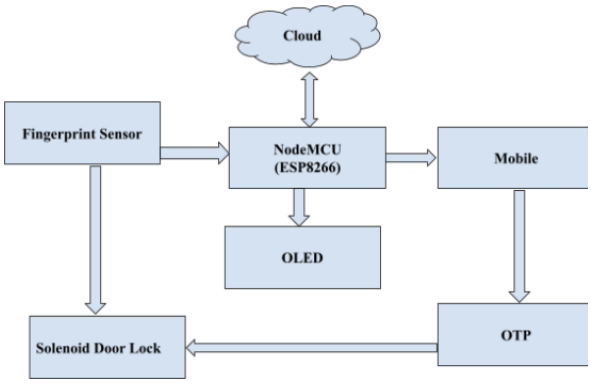

Fig: Block Diagram

An implementation plan is developed, delineating the steps, timeline, resources, and responsibilities for deploying the banking locker security system. This includes procurement, installation, integration, staff training, and testing. Thorough testing and validation follow, ensuring the system meets specified requirements and functions effectively. Simulated scenarios, penetration testing, and user acceptance testing identify and address any issues or vulnerabilities. Deployment is executed in adherence to the implementation plan, potentially employing phased deployment to minimize operational disruptions. Comprehensive training is provided to bank staff on system operation, management, security protocols, and best practices. Concurrently, awareness campaigns emphasize the importance of security and compliance in safeguarding assets and preserving customer trust. Post-deployment, monitoring and maintenance procedures are established to ensure ongoing effectiveness, reliability, and compliance. Regular inspections, software updates, equipment upgrades, and audits are conducted to identify and address security risks or vulnerabilities. A continuous improvement framework is implemented, facilitating innovation based on feedback, insights, and emerging trends in banking security. Regular reviews, stakeholder input, and exploration of new technologies contribute to the ongoing enhancement of security, efficiency, and customer satisfaction over time.

CONCLUSION In this paper, the design and implementation of a prototype of an automated vault door locking system is presented which warrants double layer of security. It ensures the proper user of the vault by securing the door with numeric password and biometric authentication. It monitors the conditions of operation of the vault from both the inside and the outside by employing several sensors which are continuously feeding information to the controller of the proposed system to confirm the robustness in terms of rightful access and security of the contents within

ISSN2454-9940

www.ijsem.org

Vol 18, Issue.2 April 2024

the vault. The entire system can be easily managed with all the status updates being reeled by the controller to the administrators eliminating the unforced reasons of human errors. The future enhancement to this work could be done by adding some more aspects. Therefore it improved the reliability of bank locker and unauthorized access will be minimized. The enhancement could be further applied to identify the illegal entrance

REFERENCES

[1] Sanal Malhotra, "Banking Locker System With Odor Identification & Security Question Using RFID GSM Technology". International Journal of Advances in Electronics Engineering – IJAEE Volume 4 : Issue 3

[2] P. Sugapriya, K. Amsavalli, "Smart Banking Security System Using Pattern Analyzer". International Journal of Innovative Research in Computer and Communication Engineering. An ISO 3297: 2007 Certified Organization Vol.3, Special Issue 8, October 2015

[3] M.P.Manjunath, P.M.Ram Kumar, Pradeep Kumar, Nalajala Gopinath, Ms. Haripriya M.E, "NFC Based Bank Locker System". International Journal of Engineering Trends and Technology (IJETT) – Volume23 Number 1- May 2015

[4] Peng-Loon Teh, Huo-Chong Ling, Soon- Nyean Cheong, "NFC Smartphone Based Access Control System Using Information Hiding," IEEE Conference on Open Systems (ICOS), December 2013.

[5] Vaijanath R. Shintre, Mukesh D. Patil, "Banking Security System Using PSoC". International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 7, July 2015

[6] Tarief M. F. Elshafiey, "Design and Implementation of a museum and bank security system using antenna as IR proximity sensor and PSoC Technology", IEEE symposium on wireless technology and applications, September 25-28 Malaysia 2011.

[7] Prof R.Srinivasan, T.Mettilda, D.Surendhran, K.Gopinath, P.Sathishkumar, "Advanced Locker Security System". International conference on Information Engineering, Management and Secuirty

[8] Roshiny Thomas, Sanjana Mathews, Sona Ojus, Sona Roselin Joseph, "Bank Locker Security System Using Face Recognition". International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE) Vol 1, Issue 5, April 2015.

ISSN2454-9940

www.ijsem.org

Vol 18, Issue.2 April 2024

[9] Ms.Geetha Hanumanthu, Mr.Dilip Chandra E, "Wireless Identification Of RFID, Fingerprint & IRIS". International journal of innovative research and development.

[10] Seshapu Prasad, D.Suneel, "Proximity Sensor Based Security Lock and Theft Detection". International journal of Science Technology and Management, Vol. No.4, Issue No.01.