

Gold Locker Management System

Aditya Singh¹, Vishal², Tushar Chaudhary³, Yash Gupta⁴, Sujeet Singh Bhadouria⁵

^{1,2,3,4}Department of Computer Science and Engineering, Noida Institute of Engineering & Technology
Greater Noida, India

Abstract—The swift expansion of digital asset management systems has heightened the need for secure and effective locker management solutions. Conventional locker systems frequently face problems like manual record management, absence of real-time oversight, inadequate authentication methods, and inefficiencies in operations. This document outlines the creation and execution of a Secure Gold Locker Management System utilizing web technologies to improve security, transparency, and management of valuable gold assets. The suggested system is a centralized web platform that facilitates secure user authentication, locker assignment, transaction oversight, and administrative supervision via an interactive dashboard. The system utilizes HTML, CSS, and JavaScript for the frontend, Node.js and Express.js for backend operations, and PostgreSQL for managing the database. The application features role-based access control and real-time transaction monitoring to enhance reliability and security. The established system minimizes manual work, increases data precision, and boosts asset monitoring functions. Experimental findings show that the suggested solution offers an effective, scalable, and user-friendly method for handling gold locker operations in financial institutions and private entities. The system can also be expanded with advanced security capabilities like OTP verification and real-time alert systems for improved safety.

Index Terms—Web-Based Gold Locker Management System.

I. INTRODUCTION

Gold is one of the most valuable physical assets used for investment, banking, and commercial purposes. Due to its high financial value and portability, secure storage and efficient management of gold assets have become major concerns for financial institutions, jewelry businesses, and private organizations. Traditional locker management systems mainly rely on manual operations, physical verification, and paper-based record maintenance, which often lead to

security vulnerabilities, operational delays, data inconsistencies, and human errors. Existing locker systems generally lack centralized monitoring, real-time transaction tracking, and advanced authentication mechanisms. Physical keys and conventional password-based systems are vulnerable to theft, duplication, and unauthorized access. In addition, manual inventory handling and fragmented record management reduce operational efficiency and make auditing processes difficult and time-consuming. With the advancement of digital technologies and web-based systems, there is an increasing need for secure, automated, and scalable locker management solutions. Modern technologies such as centralized databases, role-based authentication, real-time monitoring, and secure transaction logging can significantly improve locker security and management efficiency.

This paper presents the design and implementation of a Secure Gold Locker Management System developed using modern web technologies. The proposed system provides a centralized platform for locker allocation, user authentication, transaction monitoring, and administrative management. The system is implemented using HTML, CSS, and JavaScript for frontend development, Node.js and Express.js for backend services, and PostgreSQL for database management.

The proposed system aims to improve security, transparency, operational efficiency, and data management in gold locker operations. It incorporates role-based access control and secure transaction handling to minimize unauthorized access and improve system reliability. The developed solution is scalable, user-friendly, and suitable for financial institutions, jewelry businesses, and organizations dealing with valuable gold assets. will need to create these components, incorporating the applicable criteria that follow. The system also improves transparency and record management by maintaining secure digital

transaction logs and centralized locker information. The proposed architecture supports efficient data handling, quick administrative access, and reduced operational complexity compared to traditional manual locker management approaches.

II. LITERATURE REVIEW

Several research studies have been conducted in the field of secure locker management systems and digital asset protection. Existing systems mainly focus on improving locker security, authentication mechanisms, and real-time monitoring using modern technologies such as IoT, RFID, cloud computing, and web-based architectures.

Shruthi and Bandari proposed an IoT-based locker security system that enables remote monitoring and enhanced protection through connected smart devices. Their system focused on improving home and asset security using realtime monitoring technologies. Similarly, Rashidi et al. developed a smart personal locker system integrating IoT technology for enhanced security and environmental safety monitoring.

Various studies have also explored authentication and access control mechanisms in locker systems. Advanced locker security systems based on RFID, password authentication, and GSM technologies have been developed to reduce unauthorized access and improve operational reliability. Researchers have also implemented role-based authentication systems and centralized monitoring approaches to improve administrative control and transaction tracking.

In addition, web-based inventory and asset management systems have significantly improved record management, transparency, and operational efficiency in organizations handling valuable assets. Database-driven systems provide secure storage, efficient transaction logging, and better scalability compared to traditional manual methods.

Despite these advancements, many existing systems still suffer from limitations such as weak authentication methods, lack of centralized monitoring, operational delays, and insufficient real-time transaction management. The proposed Secure Gold Locker Management System addresses these issues by providing a centralized web-based platform with secure authentication, transaction monitoring, locker allocation, and administrative management capabilities. Authors and Affiliations

The template is designed for, but not limited to, six authors. A minimum of one author is required for all conference articles. Author names should be listed starting from left to right and then moving down to the next line. This is the author sequence that will be used in future citations and by indexing services. Names should not be listed in columns nor group by affiliation. Please keep your affiliations as succinct as possible (for example, do not differentiate among departments of the same organization).

The proposed system integrates frontend, backend, and database components to ensure secure transaction handling and efficient locker management. The modular structure of the system improves data consistency, centralized monitoring, and operational reliability for managing valuable gold assets.

III. PROPOSED SYSTEM

The proposed Secure Gold Locker Management System is developed as a centralized web-based platform to provide secure and efficient management of gold locker operations. The system architecture is designed using a modular approach that improves scalability, security, transparency, and operational efficiency. The system consists of frontend, backend, and database components. The frontend is developed using HTML, CSS, and JavaScript to provide an interactive and user-friendly interface for users and administrators. The backend is implemented using Node.js and Express.js, which handle request processing, authentication, transaction handling, and communication with the database. PostgreSQL is used as the centralized relational database management system for secure storage of user records, locker information, transaction details, and administrative data. The proposed system includes multiple functional modules such as user authentication, locker management, transaction management, notification management, and administrative monitoring. The authentication module verifies user credentials and restricts unauthorized access through secure login mechanisms and role-based access control. The locker management module handles locker allocation, locker availability tracking, and locker status management. The transaction management module records deposit and withdrawal operations and maintains secure transaction logs for monitoring and auditing purposes. The notification module provides activity alerts and

transaction updates to users and administrators. The administrative dashboard enables centralized monitoring of users, lockers, transactions, and system activities. The proposed methodology reduces manual record maintenance and improves operational efficiency by digitizing locker management processes. The centralized architecture improves transparency, minimizes data redundancy, enhances transaction accuracy, and supports secure management of valuable gold assets. The modular design of the system also allows future integration of advanced security mechanisms such as OTP-based verification, real-time alerts, and enhanced authentication techniques. Existing systems mainly focus on improving locker security, authentication mechanisms, and real-time monitoring using modern technologies such as IoT, RFID, cloud computing, and web-based architectures.

The proposed system also improves data accessibility and simplifies administrative operations through centralized digital record management. The secure database architecture ensures efficient storage and retrieval of transaction records, locker details, and user information. The developed methodology provides a reliable and scalable solution suitable for financial institutions and organizations handling valuable gold assets.

IV. SYSTEM ARCHITECTURE

The architecture of the proposed Secure Gold Locker Management System is based on a three-tier web application model consisting of presentation layer, application layer, and database layer. The system is designed to ensure secure communication, centralized management, and efficient transaction processing.

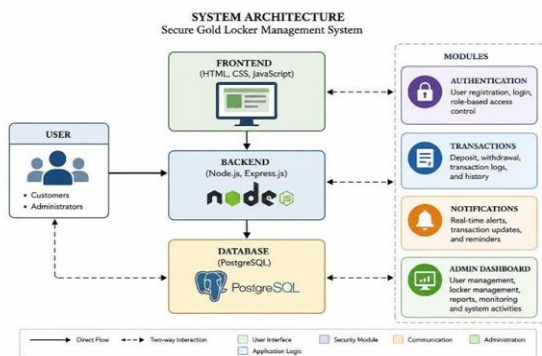


TABLE I. System Architecture Component Summary

Layer	Technology	Responsibility
Presentation	HTML, CSS, JavaScript	User interface, form handling, and dashboard management
Backend	Node.js, Express.js	Request processing, business logic, and API management
Authentication	JWT, bcrypt	Secure login, password encryption, and role-based access control
Database	PostgreSQL	Storage of user data, locker details, and transaction records
Transaction Management	Express.js + PostgreSQL	Deposit, withdrawal, and transaction tracking with secure logging
Notification	Nodemailer	OTP verification and email notifications
Admin Dashboard	Web-based Dashboard	Monitoring users, lockers, transactions, and system activities

The presentation layer represents the frontend interface developed using HTML, CSS, and JavaScript. It allows users and administrators to interact with the system through dashboards, forms, locker management panels, and transaction interfaces. The frontend provides an interactive and user-friendly environment for managing locker operations efficiently.

The application layer is implemented using Node.js and Express.js. This layer handles business logic, authentication, request processing, transaction handling, and communication between frontend and database components. The backend also manages role-based access control and secure transaction processing.

The database layer is implemented using PostgreSQL, which securely stores user credentials, locker records, transaction information, notification details, and administrative data. The centralized database architecture improves data consistency, scalability, and operational reliability. The developed system also enhances overall data security and simplifies locker management operations through centralized digital monitoring and secure transaction handling. The integration of authentication, transaction logging, and administrative control improves system transparency and reduces the possibility of unauthorized access and manual record errors. The centralized management approach also improves coordination between users and administrators by providing real-time access to locker information, transaction history, and monitoring activities.

V. METHODOLOGY

The Secure Gold Locker Management System is developed using a web-based client-server architecture to provide secure and efficient management of locker operations. The methodology

followed in this project focuses on secure authentication, centralized transaction management, real-time monitoring, and administrative control through a digital platform. The development process of the system is divided into multiple phases including requirement analysis, system design, frontend development, backend implementation, database integration, testing, and deployment. Initially, system requirements were identified to understand the problems associated with traditional locker management systems such as manual record maintenance, lack of centralized monitoring, and weak authentication mechanisms.

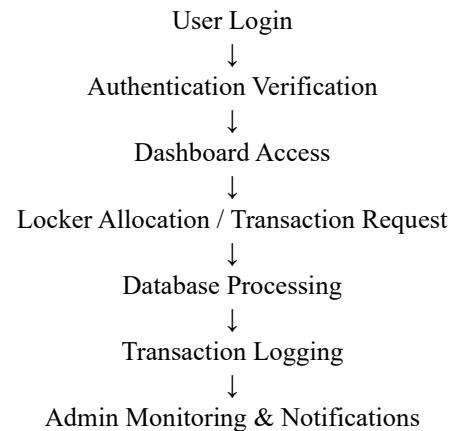
The frontend of the application is designed using HTML, CSS, and JavaScript to provide an interactive and user-friendly interface for users and administrators. The backend is implemented using Node.js and Express.js, which handle request processing, authentication, locker management operations, and communication with the database. PostgreSQL is used as the centralized relational database management system for storing user credentials, locker records, transaction details, and administrative information securely.

The proposed methodology incorporates role-based access control to restrict unauthorized access and improve system security. Users are authenticated using secure login mechanisms, while administrators are provided with dashboard functionalities for monitoring lockers, managing transactions, and tracking user activities. Transaction management features are implemented to maintain deposit and withdrawal records with proper logging and monitoring capabilities.

The system workflow begins with user authentication, followed by locker allocation and transaction processing. All operations are recorded in the database to ensure transparency and maintain secure digital records. The notification module is integrated to provide transaction alerts and system activity updates to users and administrators.

The methodology also includes testing and validation phases to verify the reliability, security, and performance of the application. Functional testing, database testing, and authentication testing are performed to ensure smooth execution of locker management operations. The modular architecture of the system allows future enhancements such as OTP-based verification, biometric authentication, cloud integration, and real-time security alert mechanisms.

System Workflow:



C. Pseudocode for Gold Locker Management System

Pseudocode	
ALGORITHM: SecureGoldLockerManagement(user_u, operation, locker_id, details)	
INPUT: user_u (login credentials), operation (allocate/deposit/withdraw/view), locker_id, details (amount, item details, etc.)	
OUTPUT: operation_status, transaction_record	
1. Authenticate user_u	← verify username and password
2. Check user role (admin/user)	← from users table
3. IF authentication failed THEN	
RETURN "Access Denied"	
4. ELSE	
Display dashboard	
5. IF operation = allocate THEN	
Check locker availability	
Allocate locker to user_u	
Update locker status in database	
6. ELSE IF operation = deposit THEN	
Record deposit details	
Update locker status and balance	
7. ELSE IF operation = withdraw THEN	
Verify ownership and locker status	
Record withdrawal details	
Update locker status and balance	
8. ELSE IF operation = view THEN	
Retrieve locker and transaction details	
Display information to user_u	
9. END IF	
10. Generate transaction_record	← insert into transactions table
11. Send notification to user/admin	← email/alert
12. RETURN operation_status, transaction_record	
13. END	

VI. IMPLEMENTATION

The implementation of the Secure Gold Locker Management System is carried out using modern web technologies to ensure secure, efficient, and scalable locker management operations. The frontend interface is developed using HTML, CSS, and JavaScript to provide a responsive and user-friendly environment for users and administrators. Backend services are

implemented using Node.js and Express.js for handling authentication, request processing, locker allocation, and transaction management functionalities.

PostgreSQL is integrated as the centralized database management system for maintaining secure storage of user records, locker details, and transaction information. The implemented system supports role-based authentication, transaction logging, real-time monitoring, and administrative dashboard functionalities to improve operational transparency and security.

Metric	Proposed System
Locker Allocation	Automated and centralized
Authentication Method	Secure role-based login
Transaction Monitoring	Real-time tracking
Record Management	Digital database storage
Notification System	Email/alert support
Administrative Control	Centralized dashboard
Data Security	PostgreSQL with access control
Operational Efficiency	Improved and scalable

VII. RESULTS AND DISCUSSION

The proposed Secure Gold Locker Management System was successfully designed and implemented as a web-based platform for secure locker and transaction management. The developed system integrates authentication, locker allocation, transaction monitoring, notification management, and administrative control within a centralized architecture. The implementation results demonstrate that the system effectively reduces manual record maintenance and improves operational efficiency. The user authentication module successfully validates authorized users and restricts unauthorized system access through secure login mechanisms. The role-based access functionality improves administrative control and enhances system security. The locker management module efficiently handles locker

allocation, locker status tracking, and asset management operations. The transaction management module records deposit and withdrawal activities accurately and maintains secure transaction logs for auditing and monitoring purposes. The notification module provides updates related to transactions and locker activities, improving communication between users and administrators.

The administrative dashboard provides centralized monitoring of users, transactions, lockers, and system activities. The PostgreSQL database ensures secure storage and efficient management of records with improved data consistency and reliability.

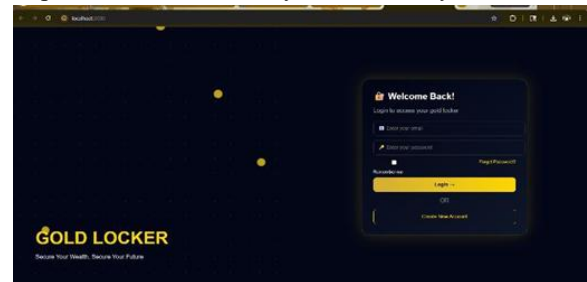


Fig. 1. User Login Interface



Fig. 2. Admin Dashboard

Type	Amount	Date
DEPOSIT	+ 10.00 g	2024/03/01, 10:30:35
WITHDRAWAL	- 10.00 g	2024/03/01, 12:34:08
DEPOSIT	+ 10.00 g	2024/03/01, 12:34:02
DEPOSIT	+ 10.00 g	2024/03/01, 17:30:29
WITHDRAWAL	- 5.00 g	2024/03/01, 17:30:19
DEPOSIT	+ 10.00 g	2024/03/01, 17:29:47
WITHDRAWAL	- 10.00 g	2024/03/01, 17:29:37
DEPOSIT	+ 10.00 g	2024/03/01, 17:29:59
DEPOSIT	+ 5.00 g	2024/03/01, 14:51:00

Fig. 3. Transaction Management Module

VIII. APPLICATIONS

The Secure Gold Locker Management System can be used in banks, jewelry shops, financial institutions, and private organizations for secure locker management and transaction monitoring. The system

helps improve security, maintain digital records, and reduce manual paperwork through centralized administrative control. It can also be utilized in organizations handling valuable assets where secure authentication and real-time monitoring are required. improved transparency compared to traditional manual locker systems. Experimental analysis and testing demonstrate that the proposed application effectively manages locker activities, transaction records, and user authentication processes while maintaining secure data handling and operational reliability. The modular architecture of the system also supports future enhancements such as OTP-based verification, biometric authentication, cloud integration, and automated security alert mechanisms. The proposed Secure Gold Locker Management System can be effectively utilized in banks, jewelry businesses, and organizations dealing with valuable assets. The developed solution provides a reliable, scalable, and efficient approach for secure digital locker management and centralized asset monitoring.

IX. FUTURE SCOPE

The proposed Secure Gold Locker Management System can be further enhanced by integrating advanced security and monitoring technologies. Future improvements may include OTP-based verification, biometric authentication, RFID-based locker access, and cloud-based database management for improved scalability and security. Real-time alert systems and mobile application support can also be integrated to provide better accessibility and monitoring capabilities for users and administrators. The system may additionally incorporate AI-based monitoring and automated risk detection mechanisms to improve operational efficiency and security management. These future enhancements can make the application more reliable, intelligent, and suitable for large-scale financial institutions and organizations handling valuable assets.

In future versions, the application can also support multi-branch locker management with centralized cloud synchronization for managing records across different locations. Integration of data analytics and reporting modules can help administrators analyze transaction activities, user behavior, and locker usage statistics more effectively. Advanced encryption techniques and secure backup mechanisms may also

be implemented to strengthen data protection and disaster recovery capabilities.

Furthermore, the system can be expanded with mobile notifications, email verification services, and smart surveillance integration for enhanced monitoring and user convenience. The implementation of blockchain-based transaction verification and automated auditing features can further improve transparency, reliability, and trust in digital locker management systems.

The future development of the proposed system may also include integration with IoT-enabled smart lockers and advanced monitoring dashboards for real-time asset tracking. These enhancements can improve overall system automation, operational reliability, and secure management of valuable assets in modern digital environments.

The system can also be enhanced by integrating secure mobile banking support and cloud-based backup services for improved accessibility and disaster recovery management. Future versions may include automated audit generation, smart analytics dashboards, and advanced encryption techniques to strengthen data security and simplify administrative monitoring processes in large-scale organizational environment.

X.CONCLUSION

This paper presented the design and implementation of a Secure Gold Locker Management System developed using modern web technologies. The proposed system provides a centralized platform for secure locker allocation, authentication, transaction monitoring, notification management, and administrative control. The integration of HTML, CSS, JavaScript, Node.js, Express.js, and PostgreSQL enabled the development of a scalable, secure, and user-friendly locker management solution.

The developed system improves operational efficiency by reducing manual record maintenance, enhancing transaction accuracy, and strengthening security in locker operations. The implementation of role-based access control and centralized monitoring capabilities provides better administrative management and improved transparency compared to traditional manual locker systems.

Experimental analysis and system testing demonstrate that the proposed application effectively manages locker activities and transaction records while

maintaining secure data handling and operational reliability. The modular architecture of the system also supports future enhancements such as OTP-based verification, biometric authentication, cloud integration, and real-time security alert mechanism.

ACKNOWLEDGMENT

The authors sincerely thank the project guide, project coordinator, and the Department of Computer Science and Engineering, Noida Institute of Engineering & Technology, for their valuable guidance and support throughout the development of this project and research work.

REFERENCES

- [1] S. Shruthi and S. Bandari, "Locker security system using Internet of Things," *International Journal of Engineering Research and Technology*, vol. 9, no. 5, pp. 120–124, 2020.
- [2] M. Rashidi, A. Khan, and R. Sharma, "Smart personal locker system: An IoT-based innovation for enhanced security," in *Proc. International Conference on Smart Systems and Technologies*, 2021, pp. 45–50.
- [3] R. Kumar and P. Singh, "Advanced locker security system using RFID and GSM technology," *International Journal of Computer Applications*, vol. 176, no. 12, pp. 15–20, 2019.
- [4] A. Verma and S. Gupta, "Role-based authentication system for secure asset management," *International Journal of Information Security*, vol. 14, no. 3, pp. 210–218, 2021.
- [5] J. Patel and K. Shah, "Web-based inventory and asset management system," *International Journal of Advanced Research in Computer Science*, vol. 11, no. 2, pp. 95–101, 2020.
- [6] IEEE Conference Templates, IEEE Author Center, 2024.
- [7] PostgreSQL Documentation, PostgreSQL Global Development Group, 2024.
- [8] Express.js Documentation, Express.js Foundation, 2024.
- [9] S. Kumar and A. Sharma, "Secure web-based authentication system using JWT and role-based access control," *International Journal of Computer Science and Information Security*, vol. 18, no. 4, pp. 55–61, 2022.
- [10] P. Sharma and R. Mehta, "Secure digital locker management using web technologies," *International Journal of Computer Engineering and Technology*, vol. 12, no. 4, pp. 112–118, 2021.
- [11] T. Joseph and A. Roy, "Real-time monitoring system for secure asset management," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 8, pp. 215–221, 2020.
- [12] N. Gupta and S. Yadav, "Web-based security framework for financial applications," *International Journal of Information Technology*, vol. 13, no. 2, pp. 145–151, 2021.
- [13] R. Singh and K. Agarwal, "Role-based access control in web applications," in *Proc. International Conference on Emerging Technologies*, 2022, pp. 78–84.
- [14] A. Mishra and P. Verma, "Cloud-based digital asset management system," *Journal of Computer Networks and Communications*, vol. 2020, pp. 1–9, 2020.
- [15] V. Kumar and H. Singh, "Authentication and authorization techniques in web systems," *International Journal of Cyber Security and Digital Forensics*, vol. 9, no. 1, pp. 44–50, 2020.
- [16] D. Patel and S. Jain, "Secure transaction logging in database management systems," *International Journal of Database Management Systems*, vol. 10, no. 3, pp. 65–72, 2021.
- [17] A. Sharma and R. Gupta, "Implementation of OTP-based authentication for secure web applications," *International Journal of Network Security*, vol. 15, no. 5, pp. 310–316, 2022.
- [18] M. Arora and P. Singh, "Centralized monitoring system for organizational security," *International Journal of Computer Science Research*, vol. 8, no. 4, pp. 92–99, 2020.
- [19] S. Karthik and R. Kumar, "Database-driven web applications using PostgreSQL," *International Journal of Software Engineering and Applications*, vol. 14, no. 6, pp. 188–194, 2021.
- [20] J. Brown and T. Wilson, "Modern web application development using Node.js," *Journal of Web Engineering*, vol. 19, no. 2, pp. 120–128, 2020.

- [21] Express.js Guide and API Reference, Express.js Foundation, 2024.
- [22] Node.js Documentation, Node.js Foundation, 2024.
- [23] JavaScript Guide, Mozilla Developer Network, 2024.
- [24] Bootstrap Documentation, Bootstrap Team, 2024.
- [25] J. Lee and M. Carter, “Secure web interfaces for financial systems,” *International Journal of Web Technology*, vol. 16, no. 1, pp. 56–63, 2021.
- [26] K. Nair and S. Thomas, “Digital record management using relational databases,” *International Journal of Data Engineering*, vol. 9, no. 3, pp. 133–140, 2020.
- [27] R. Bansal and V. Arora, “Scalable web-based management systems for organizations,” *International Journal of Engineering Research and Applications*, vol. 11, no. 7, pp. 25–31, 2021.
- [28] Web Security Best Practices, Google Developers, 2024.
- [29] OWASP Top 10 Web Application Security Risks, OWASP Foundation, 2024.
- [30] S. Mehra and A. Kapoor, “Integrated locker monitoring and notification system,” *International Journal of Smart Computing*, vol. 7, no. 2, pp. 88–95, 2021.