International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

A Secure Blockchain-Integrated Jewellery Management System Using IPFS-Based Decentralized Storage and Encrypted Communication

K. Sharmila Reddy[1*], Gandu Rithika[2], Gorre Vikas[2], Bandari Vyshnavi[2], Dunna Shankar[2]

[1]Associate Professor & Head, [2]UG Student, [1,2]Department of Computer Science and Engineering

[1,2]Vaagdevi Engineering College, Bollikunta, Warangal, 506005, Telangana, India.

*Correspondence: K. Sharmila Reddy (sharmilakreddy@gmail.com)

ABSTRACT

The jewellery transaction and management system plays a crucial role in ensuring secure communication, data integrity, and efficient coordination between customers, jewellery owners, and administrators. Traditionally, such systems relied on manual record-keeping, paper-based documentation, and unsecured digital communication methods. These conventional approaches were time-consuming, prone to human errors, lacked transparency, and were highly vulnerable to data tampering, unauthorized access, and information loss. There was no reliable mechanism to ensure data integrity or traceability of user actions. The proposed system introduces a secure, web-based application developed using the Flask framework, integrating advanced security and data management techniques. The system incorporates encryption mechanisms using the Hill Cipher algorithm for secure message exchange and file protection. Additionally, a hybrid blockchain architecture is implemented using Inter-Planetary File System (IPFS) through Pinata, where each user activity is stored as a hash-linked block, ensuring tamper-resistant and immutable data storage. Real-time functionalities such as gold price updates are integrated using WebSocket communication, enhancing user interaction. The system also utilizes Tiny Data Base (TinyDB) for lightweight database management and Secure Hash Algorithm (SHA-256) hashing for maintaining block integrity. The research is completed by integrating user authentication, OTP-based verification, encrypted communication, blockchain-based logging, and secure file handling into a unified platform. This approach ensures improved security, transparency, and reliability compared to traditional systems, providing a robust and scalable solution for modern digital jewellery transaction management.

Keywords: Jewellery Transaction System, Flask Framework, Hill Cipher, Blockchain, InterPlanetary File System (IPFS), Pinata, SHA-256, TinyDB.

1. INTRODUCTION

The rapid digital transformation of the jewellery industry has led to a strong dependence on web-based platforms for managing high-value assets, ownership records, certification documents, and customer interactions, as illustrated in Fig. 1. Industry reports highlight a continuous shift toward digital inventory management and online transaction processing, resulting in the generation and exchange of large volumes of sensitive data. With the expansion of online jewellery marketplaces and digital submission systems, organizations are required to securely handle critical information such as valuation details, identity records, and transaction histories within digital infrastructures. This growing reliance on interconnected technologies has intensified concerns regarding data confidentiality, integrity, and access control. Research in cybersecurity emphasizes that industries dealing with valuable assets and financial transactions face a higher risk of data breaches and unauthorized access, underscoring the need for robust and secure digital solutions.

Received: 28-02-2026 | Accepted: 02-04-2026 | Published: 10-04-2026

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

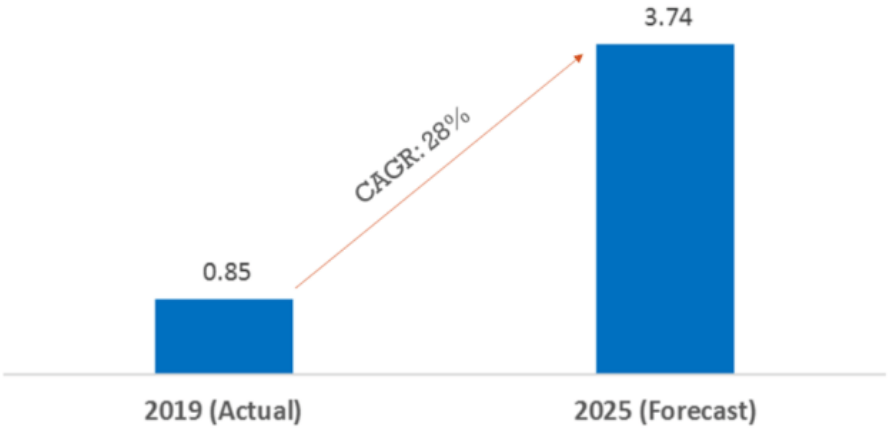

Fig. 1: Indian online jewellery market

Contemporary jewellery management ecosystems involve multiple stakeholders including administrators, asset owners, verification authorities, and customers operating within shared digital infrastructures. Such multi-role environments require structured coordination mechanisms to ensure accurate data handling, traceable workflow progression, and secure communication channels. Regulatory compliance standards and consumer trust expectations further demand strict control over how confidential information is processed, accessed, and archived. Without strong access management and encryption enforcement, sensitive asset-related data becomes vulnerable to unauthorized viewing, manipulation, or unintended disclosure. The operational scale of digital platforms also necessitates reliable logging and monitoring mechanisms to maintain accountability and transparency.

The adoption of cloud-integrated applications and centralized workflow platforms has improved operational efficiency but simultaneously introduced security complexities. Real-time communication modules, file exchange systems, and remote access capabilities increase the importance of cryptographic safeguards to protect information during both transmission and storage. Research in application security highlights that improper encryption implementation and weak authorization policies remain major contributors to confidentiality breaches in web-driven systems. Therefore, structured digital architectures that integrate secure communication protocols, encrypted data storage, controlled role-based access, and systematic monitoring are critical for sustaining secure and reliable jewellery submission and resolution environments. Such architectures ensure not only protection of sensitive information but also enhanced workflow traceability and operational resilience in high-value digital ecosystems.

2. LITERATURE SURVEY

Sternad Zabukovšek, et al. [1] used the Process and Enterprise Maturity Model (PEMM) to assess the organization's maturity level concerning the Document management systems (DMS) life cycle. Findings are presented from the research study. The research study was based on a questionnaire and collected data from DMS users. The research study showed that an organization's maturity impacts the DMS' life cycle. Organizations that manage the DMS' life cycle will better cope with digital transformation and sustainability issues related to paperless business. Li, et al. [2] defined the model, divides roles into abstract roles and specific roles, and designs the operating process of the access control model. The model had four characteristics: support role name repetition, platform–domain isolation management, inter-domain isolation management, and fine-grained cross-domain sharing. By establishing security violation formulas for security analysis, it is finally shown that role-based access

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

control model for inter-system cross-domain in multi-domain environment (RBAC-IC) can operate safely. Bucko, et al. [3] presented a solution to enhance the trustworthiness of user authentication in web applications based on their behavior history. The solution considers factors such as the number of password attempts, IP address consistency, and user agent type and assigns a weight or percentage to each.

Akuthota, et al. [4] investigated how RBAC has transformed from a traditional access control mechanism into an AI-enhanced security framework capable of addressing contemporary cloud security challenges. Through examination of real-world implementations, the article demonstrates RBAC's effectiveness in reducing security incidents, streamlining administrative processes, and ensuring regulatory compliance Gunjal, et al. [5] presented a secure data sharing approach, which, by utilizing Role-Based Access Control and the AES encryption method, is capable of achieving secure key distribution & information sharing for dynamic groups. The data is protected by our system, which also allows for its regeneration in the event that it is mishandled by an unauthorized user. Nafiseh Soveizi, et al. [6] presented the state-of-the-art security solutions organized according to the phases of the workflow life cycle they target for both business and scientific workflows. The analysis shows that most of the existing literature focuses on the modeling and execution phases, while the monitoring and adaptation phases are not covered adequately by a scarce amount of publications thus leaving a huge gap in the body of knowledge relevant to detection, prevention of and reaction to security violations in cloud-based workflows.

Xi, et al. [7] enhanced the security of the traditional Hill cipher (THC) and expand its application in medical image encryption, a novel dynamic Hill cipher with Arnold scrambling technique (DHCAST) is proposed in this work. Unlike the THC, the proposed DHCAST uses a time-varying matrix as its secret key, which greatly increases the security of the THC, and the new DHCAST is successfully applied in medical images encryption Mfungo, et al. [8] presented a new image encryption technique that combines the Kronecker xor product, Hill cipher, and sigmoid logistic Map. Their proposed algorithm begins by shifting the values in each row of the state matrix to the left by a predetermined number of positions, then encrypting the resulting image using the Hill Cipher Lone, et al. [9] showed that the scheme is vulnerable to brute force attacks and lacks both Shannon's primitive operations of cryptography and Kerckchoff's principle. To circumvent these limitations, an efficient modification to the existing scheme is proposed using an affine Hill cipher in combination with ECC and a 3D chaotic map.

Joseph, et al. [10] developed a system to computerize the major transactions in jewellery like, purchases, sales and bill preparation. This software can be used for managing customers as well as employees associated with that shop in a short period of time. Sanil Gandhi, et al. [11] presented a novel Blockchain-based Approval Process System (BAPS) to establish mutual trust between the submitter and the approving authorities. The proposed system's design, implementation, and evaluation are included in this paper. The suggested approach can shorten the time needed to obtain the permissions and increase transparency between the users and the authority. In addition, it eliminates issues such as the misplacement of papers. Chowdhary, et al. [12] proposed an analysis for performing image encryption and decryption by hybridization of Elliptic Curve Cryptography (ECC) with Hill Cipher (HC), ECC with Advanced Encryption Standard (AES) and ElGamal with Double Playfair Cipher (DPC). This analysis is based on the following parameters: (i) Encryption and decryption time, (ii) entropy of encrypted image, (iii) loss in intensity of the decrypted image, (iv) Peak Signal to Noise Ratio (PSNR), (v) Number of Pixels Change Rate (NPCR), and (vi) Unified Average Changing Intensity (UACI).

Received: 28-02-2026 | Accepted: 02-04-2026 | Published: 10-04-2026

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

3. PROPOSED METHODOLOGY

The proposed system is a secure web-based jewellery management platform designed to manage jewellery submissions, customer interactions, secure communication, encrypted file sharing, and tamper-resistant activity tracking as demonstrate in Fig. 2. The system connects three major user roles, namely administrator, jewellery owner, and customer, within a unified digital environment. It is developed using the Flask framework and integrates security mechanisms such as OTP verification, Hill Cipher encryption, IPFS with Pinata, SHA-256 hashing, TinyDB storage, and WebSocket-based real-time updates. The system replaces traditional manual handling of jewellery records and communication with a structured, automated, and secure workflow.

Fig. 2: Proposed system architecture

User Registration and Role Selection: The system allows new users to register as either a customer or a jewellery owner. During registration, the user provides the required details such as name, email, password, phone number, and address. Jewellery owners also provide additional business-related details. The entered information is stored temporarily until verification is completed.

OTP-Based Email Verification: After registration, the system generates a One-Time Password and sends it to the registered email address. The user enters the OTP for verification. Once the OTP is validated, the account is created successfully and marked for administrator approval. This step strengthens account authenticity and prevents unauthorized registration.

Administrator Approval of Accounts: The administrator reviews newly registered users and approves valid accounts. Only approved users are permitted to log in and access the system. This approval mechanism provides controlled access and ensures that unknown or invalid users are restricted.

Secure User Login and Role-Based Access: After approval, users log in using their credentials. The system verifies the email and password using secure password hashing. Based on the assigned role, the user is redirected to the appropriate dashboard. The administrator manages users and submissions, the jewellery owner manages item submissions and secure communication, and the customer browses approved jewellery items and interacts with the system.

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

Jewellery Submission by Owner: The jewellery owner submits item details such as title, description, jewellery type, weight, material, and estimated value. These submissions are stored in the database with pending status. This step digitizes the process of item registration and reduces dependence on manual records.

Submission Verification and Approval by Administrator: The administrator examines the submitted jewellery information and either approves or rejects the submission. Approved items become visible to customers for browsing and purchase interest. Rejected items are stored with proper status updates and remarks. This step maintains data reliability and administrative control.

Customer Browsing and Purchase Request: Customers view all administrator-approved jewellery items through the system dashboard. When a customer shows interest in an item, the purchase process is initiated. The system automatically sends email notifications to both the customer and the jewellery owner with the relevant item and contact details. This establishes secure and direct communication regarding the transaction.

Secure Communication Between Users: The system provides a communication module through which jewellery owners, customers, and administrators exchange messages. Users choose encrypted communication for sensitive content. In such cases, the message is encrypted using the Hill Cipher algorithm before storage. Authorized users later decrypt the message when needed. This protects confidential communication within the platform.

Secure File Upload and Encrypted Sharing: Jewellery owners upload documents or files related to jewellery items and share them with customers. Before storage, file contents are encrypted using the file encryption functions. The encrypted file is stored securely, and authorized customers download either the encrypted version or the decrypted version based on access rights. This step ensures secure transmission and storage of valuable digital documents.

Customer Profile and Image Upload: Customers manage their profile details and upload jewellery-related images for reference or communication purposes. Uploaded images are stored with unique file names, linked to the user account, and managed through the profile module. This improves personalization and record management.

Gold Price Monitoring in Real Time: The system integrates a gold price service to provide current gold price information. Real-time gold price updates are delivered using WebSocket communication. This feature keeps users informed about live price changes and improves practical decision-making during jewellery-related transactions.

Blockchain-Based Activity Logging: Every major action performed in the system, such as user registration, login, jewellery submission, purchase initiation, message sending, password reset, and file handling, is logged. A block is created containing timestamp, user details, action details, previous IPFS hash, and a SHA-256 block hash. This structure forms a linked blockchain-style record.

IPFS Storage with Pinata Integration: Each generated block is uploaded to IPFS through Pinata. After successful upload, the returned IPFS hash is stored locally along with metadata for retrieval. The current block retains the reference to the previous block using the previous IPFS hash field. This process creates a tamper-resistant and traceable activity history, strengthening transparency and integrity.

Local Metadata Management Using TinyDB: While block data and files are secured externally and internally, TinyDB is used to manage local application data such as users, submissions, messages,

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

feedback, files, images, logs, and reset tokens. This lightweight database supports efficient storage and retrieval within the web application.

Password Recovery and Secure Reset: In case a user forgets the password, the system provides a secure password reset mechanism. An OTP is sent to the registered email address, and after successful verification, a unique token-based reset link is generated. The new password is stored only after hashing, which improves account recovery security.

Report Generation and Monitoring by Administrator: The administrator accesses dashboards for monitoring total users, jewellery owners, customers, submissions, pending items, resolved records, logs, and blockchain activity. This provides an overall view of system operation and supports efficient management.

Pinata

Pinata is a cloud-based IPFS pinning service that ensures reliable and persistent storage of data on the IPFS network. It simplifies the process of uploading, managing, and retrieving files or JSON data without requiring users to run their own IPFS nodes. By pinning data, Pinata guarantees that the stored content remains continuously available and accessible through IPFS gateways as shown in Fig. 3. In the proposed system, Pinata is used to upload blockchain blocks and encrypted files, ensuring secure, immutable, and permanent storage of system activities.

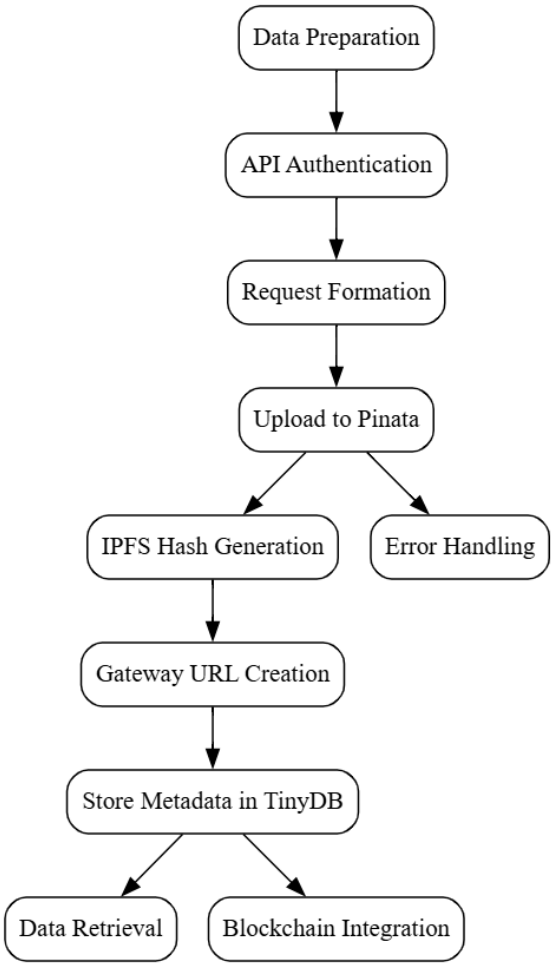

Fig. 3: Internal working of pinata.

Received: 28-02-2026 | Accepted: 02-04-2026 | Published: 10-04-2026

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

Data Preparation: When a block or file is ready for storage, the system prepares the data in a structured format. This includes blockchain block data or encrypted file content along with metadata such as timestamp and action type. Proper formatting ensures smooth communication with the Pinata API.

API Authentication Setup: The system uses Pinata API keys and secret keys to authenticate requests. These credentials are included in the request headers to establish a secure connection. This step ensures that only authorized applications interact with the Pinata service.

Request Formation: A POST request is created using the Pinata API endpoint for uploading data. The payload includes the content to be stored and metadata such as a unique name for identification. This structured request prepares the data for transmission to the IPFS network.

Data Upload to Pinata: The system sends the prepared request to Pinata using HTTP protocols. Pinata processes the request and pins the data onto the IPFS network. This step ensures decentralized storage and availability of the uploaded content.

IPFS Hash Generation: After successful upload, Pinata returns a unique IPFS hash (CID) for the stored data. This hash acts as the permanent address of the content in the IPFS network. It is used for accessing and verifying the stored data.

Gateway URL Creation: Pinata provides a gateway URL that allows easy retrieval of the stored content through a web browser. This URL is constructed using the returned IPFS hash. It simplifies access without requiring direct interaction with IPFS nodes.

Local Metadata Storage: The system stores the IPFS hash, gateway URL, metadata name, timestamp, and other details in TinyDB. This local storage allows efficient tracking and retrieval of uploaded records. It also supports faster access within the application.

Data Retrieval: Whenever required, the system uses the IPFS hash or gateway URL to fetch the stored data. The retrieved content matches exactly with the original uploaded data due to content-based addressing. This ensures data integrity and consistency.

Error Handling and Fallback: If the upload to Pinata fails due to network or API issues, the system generates a local hash as a fallback reference. This ensures that the system continues to function without interruption. It maintains reliability even under failure conditions.

Integration with Blockchain Logging: The uploaded data is linked with the blockchain mechanism by storing the IPFS hash as part of the block reference. This creates a connection between blockchain records and IPFS storage. It ensures tamper-resistant, traceable, and secure data management.

4. Results Description

Fig. 4 depicts the user management screen that allows administrators to oversee registered accounts within the platform. The figure illustrates the structured presentation of user details, assigned roles, and account information. It represents the administrative control mechanism for maintaining authorization and data integrity. The screen demonstrates how the system supports account lifecycle management and role-based permissions.

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

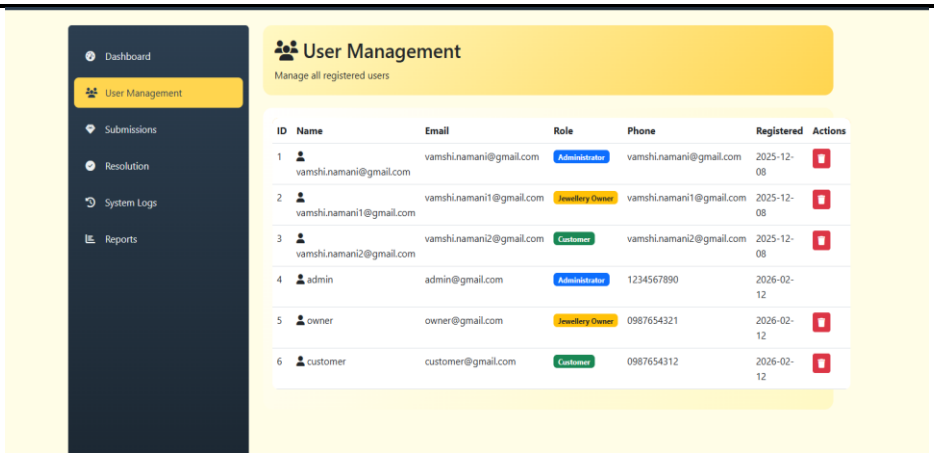

Fig. 4: User management

Fig. 5 illustrates the jewellery submissions overview screen where submitted records are reviewed and monitored. The figure depicts structured information related to jewellery attributes, ownership details, and processing status. It represents the evaluation stage of the workflow where administrative review and verification occur. The screen demonstrates how submissions are organized for efficient tracking and decision-making.

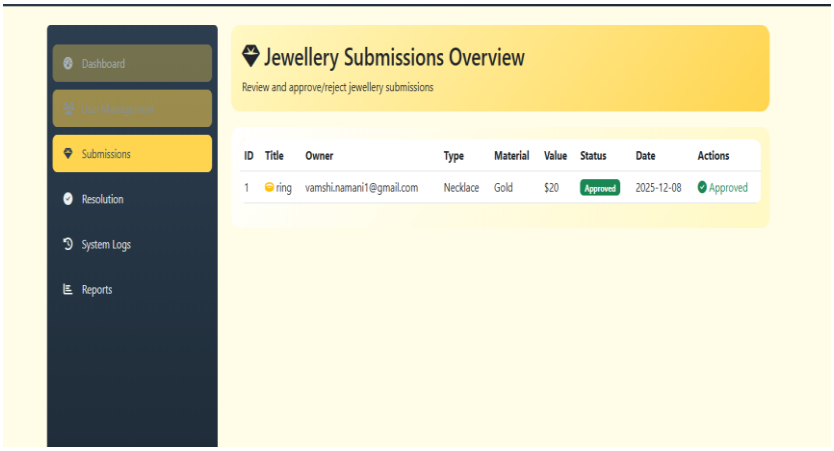

Fig. 5: Jewellery submission overview

Fig. 6 illustrates the jewellery request submission interface that enables owners to create new entries within the system. The figure depicts the structured data input process for recording jewellery attributes and related details. It represents the initiation stage of the workflow lifecycle. The screen demonstrates how standardized data capture supports organized processing and database integration.

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

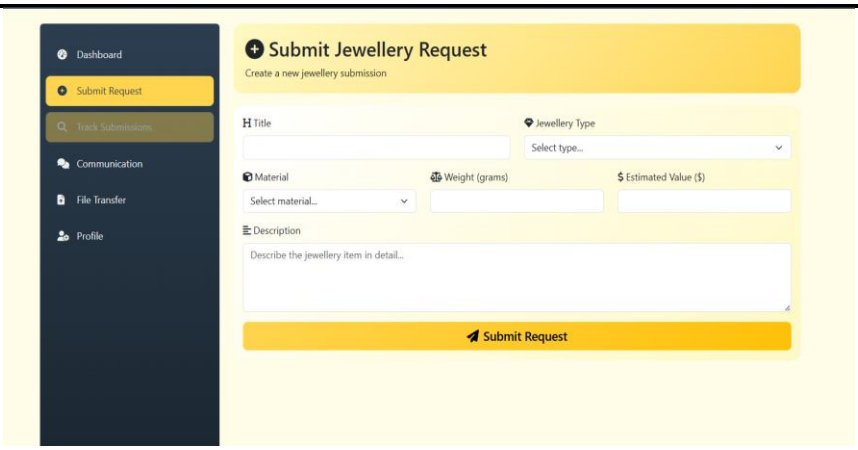

Fig. 6: Submitting request

Fig. 7 depicts the track submissions screen that allows users to monitor the status of previously submitted jewellery items. The figure illustrates how submission information and progress indicators are presented for user reference. It represents the tracking mechanism within the workflow system. The screen demonstrates transparency in submission handling and approval processes.

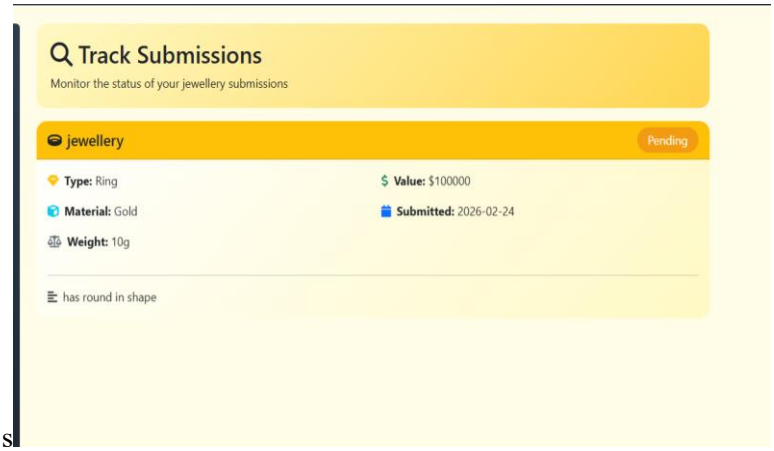

Fig. 7: Track submissions.

Fig. 8 depicts the secure file transfer screen that facilitates encrypted file sharing between users. The figure illustrates the controlled upload and sharing process implemented within the workflow. It represents the secure data exchange mechanism responsible for protecting sensitive documents. The screen demonstrates integration of encryption techniques for maintaining file confidentiality.

Received: 28-02-2026 | Accepted: 02-04-2026 | Published: 10-04-2026

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

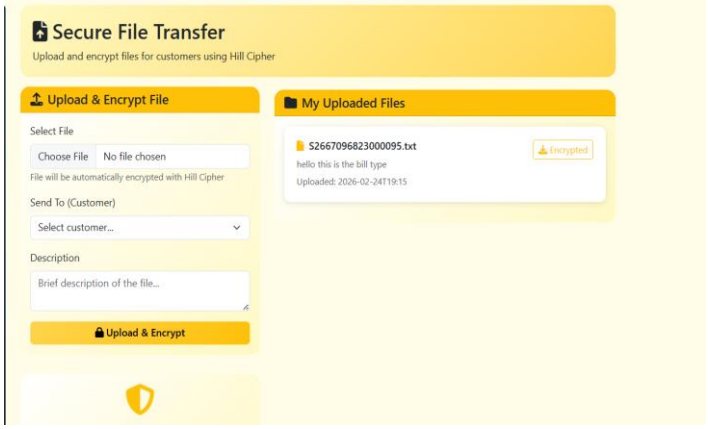

Fig. 8: Secure file transfer.

Fig. 9 illustrates the profile management interface where users update and maintain personal account information. The figure depicts the structured environment for editing user details within the system. It represents the identity management component that supports accurate record maintenance. The screen demonstrates how user information is synchronized with RBAC structures.

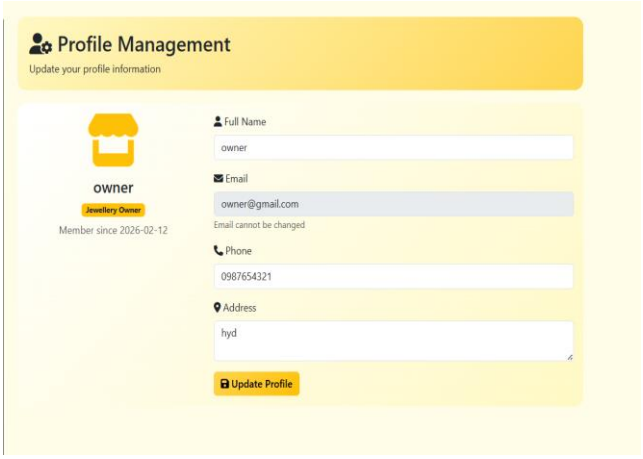

Fig. 9: Profile management

Fig. 10 depicts the track resolution status screen that allows monitoring of submission outcomes across different workflow stages. The figure illustrates categorized resolution indicators reflecting processing progress. It represents the reporting and monitoring layer of the system. The screen demonstrates structured visualization of submission statuses and resolution notes.

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

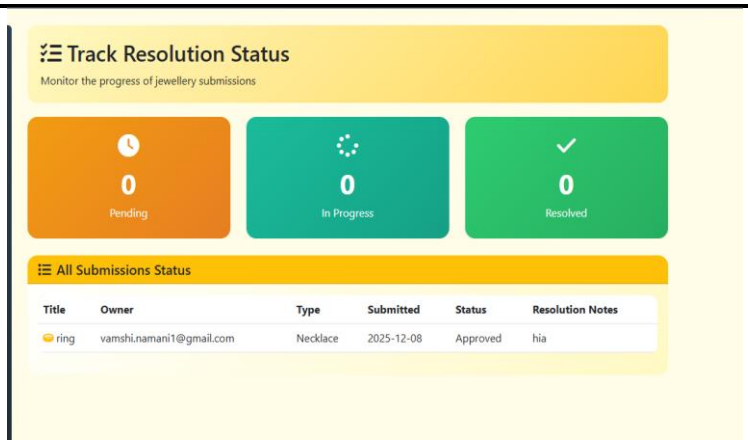

Fig. 10: Track resolution status screen

Fig. 11 illustrates the received files interface where users access encrypted documents shared through the platform. The figure depicts secure retrieval options for downloading encrypted content or performing decryption. It represents the final stage of protected file exchange within the workflow. The screen demonstrates controlled access to shared digital assets using implemented security mechanisms.

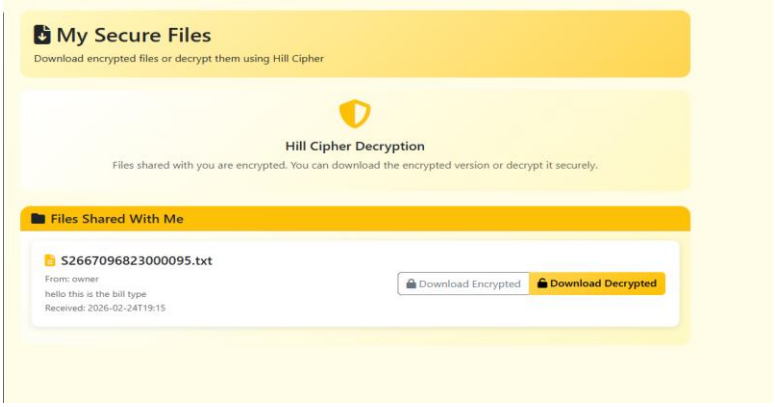

Fig. 11: Received files screen

5. Conclusion

The developed system successfully integrates secure communication, role-based access control, blockchain-based logging, and encrypted file handling within a unified Flask-based web application. By combining OTP-based authentication, TinyDB storage, and encryption techniques such as the Hill Cipher, the system establishes a secure environment for managing jewellery submissions, user interactions, and administrative operations. The inclusion of decentralized storage using IPFS with Pinata enhances data integrity and ensures tamper-resistant storage of system activities. The implementation of role segregation, including administrator, jewellery owner, and customer, ensures controlled access and secure data handling across all system modules. Blockchain-style logging using SHA-256 hashing provides transparency and traceability by linking user actions into an immutable chain. The integration of WebSocket communication for real-time gold price updates improves system responsiveness and user experience. From a performance perspective, the system demonstrates efficient data handling through lightweight TinyDB storage and optimized Flask routing. Workflow automation for user approval, jewellery submission, and transaction processing reduces manual effort and improves operational speed. Encrypted messaging and secure file sharing maintain confidentiality without affecting performance. Overall, the system delivers a secure, scalable, and reliable solution for digital

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

jewellery management by integrating encryption, decentralized storage, real-time communication, and blockchain-inspired auditing within a single platform.

REFERENCES

[1] Sternad Zabukovšek, S.; Jordan, S.; Bobek, S. Managing Document Management Systems' Life Cycle in Relation to an Organization's Maturity for Digital Transformation. Sustainability 2023, 15, 15212. https://doi.org/10.3390/su152115212

[2] Li, Y.; Du, Z.; Fu, Y.; Liu, L. Role-Based Access Control Model for Inter-System Cross-Domain in Multi-Domain Environment. Appl. Sci. 2022, 12, 13036. https://doi.org/10.3390/app122413036

[3] Bucko, A.; Vishi, K.; Krasniqi, B.; Rexha, B. Enhancing JWT Authentication and Authorization in Web Applications Based on User Behavior History. Computers 2023, 12, 78. https://doi.org/10.3390/computers12040078

[4] Akuthota, Arun. (2025). Role-Based Access Control (RBAC) in Modern Cloud Security Governance: An In-depth Analysis. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 11. 3297-3311. 10.32628/CSEIT25112793.

[5] Gunjal, M. B. ., & Sonawane, V. R. . (2023). Multi Authority Access Control Mechanism for Role Based Access Control for Data Security in the Cloud Environment. *International Journal of Intelligent Systems and Applications in Engineering*, *11*(2s), 250 –. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2623

[6] Nafiseh Soveizi, Fatih Turkmen, Dimka Karastoyanova, Security and privacy concerns in cloud-based scientific and business workflows: A systematic review, Future Generation Computer Systems, Volume 148, 2023, Pages 184-200, ISSN 0167-739X, https://doi.org/10.1016/j.future.2023.05.015.

[7] Xi, Y.; Ning, Y.; Jin, J.; Yu, F. A Dynamic Hill Cipher with Arnold Scrambling Technique for Medical Images Encryption. Mathematics 2024, 12, 3948. https://doi.org/10.3390/math12243948

[8] Mfungo, D.E.; Fu, X.; Wang, X.; Xian, Y. Enhancing Image Encryption with the Kronecker xor Product, the Hill Cipher, and the Sigmoid Logistic Map. Appl. Sci. 2023, 13, 4034. https://doi.org/10.3390/app13064034

[9] Lone, P.N.; Singh, D.; Stoffová, V.; Mishra, D.C.; Mir, U.H.; Kumar, N. Cryptanalysis and Improved Image Encryption Scheme Using Elliptic Curve and Affine Hill Cipher. Mathematics 2022, 10, 3878. https://doi.org/10.3390/math10203878

[10] Joseph, Sunil & George, Geethu & Vazhacharickal, Prem & K.R, Reshma. (2017). Jewellery management systems: an overview.

[11] Sanil Gandhi, Arvind Kiwelekar, Laxman Netak, Shashank Shahare, A blockchain-based data-driven trustworthy approval process system, International Journal of Information Management Data Insights, Volume 3, Issue 1, 2023, 100162, ISSN 2667-0968, https://doi.org/10.1016/j.jjimei.2023.100162.

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

[12] Chowdhary, C.L.; Patel, P.V.; Kathrotia, K.J.; Attique, M.; Perumal, K.; Ijaz, M.F. Analytical Study of Hybrid Techniques for Image Encryption and Decryption. Sensors 2020, 20, 5162. https://doi.org/10.3390/s20185162