International Journal of
AI EBIOMEDICINE INNOVATIONS
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0507 www.zesterapublications.com Original Research Paper

# Cloud Database Maintenance Fee Collection with Secure Complaint Handling

Polapaka Ramyasree, G. Arpitha*

Vaagdevi Engineering College, Warangal, 506005, Telangana, India.

*Correspondence: G. Arpitha

## ABSTRACT

The widespread adoption of cloud computing has significantly increased the demand for secure storage, controlled resource access, and efficient administrative management of organisational information. Conventional cloud-based database platforms frequently depend on centralized security models that provide limited authorisation controls, insufficient activity monitoring, and inadequate protection of sensitive information. These limitations increase the possibility of unauthorised access, data misuse, and inefficient handling of administrative tasks such as maintenance fee collection, payment verification, and grievance management. To address these challenges, this paper presents a Secure Role-Based Cloud Database Maintenance Fee Collection System (CBFCS) developed using the Flask framework, Tiny Database (TinyDB), and a hybrid cryptographic architecture. The proposed solution enforces role-oriented authorization by defining separate privileges for administrators, database managers, and end users, ensuring that each user accesses only permitted resources. Sensitive documents and stored information are protected through a hybrid encryption mechanism that combines Rivest–Shamir–Adleman (RSA) for secure key exchange and Advanced Encryption Standard–Galois/Counter Mode (AES-GCM) for high-performance data encryption and integrity verification. TinyDB serves as a lightweight NoSQL repository for storing user records, encrypted file metadata, payment information, maintenance details, complaint records, and system audit logs. Furthermore, the inclusion of secure complaint processing, transaction tracking, and comprehensive auditing enhances system transparency and accountability. Experimental implementation demonstrates that the proposed framework provides stronger data protection, improved operational reliability, and scalable management for modern cloud database environments.

**Keywords:** Cloud Computing, Role-Based Access Control (RBAC), Hybrid Encryption, AES-GCM and RSA, Cloud Database Security.

## 1. INTRODUCTION

The idea behind cloud computing is to provide all possible facilities such as software, IT infrastructure, and services to its customers for use over the internet. Cloud computing systems are large-scale, heterogeneous collections of autonomous systems and flexible computational architecture. This technology is emerging, as it is considered the first choice for businesses that do not want to deal with the in-house maintenance of systems and a development team [1]. Many businesses, such as Amazon AWS, Google, IBM, Sun,

International Journal of
AI EBIOMEDICINE INNOVATIONS
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0507 www.zesterapublications.com Original Research Paper

Microsoft, and many others, are developing efficient cloud products and technology [2]. In cloud technology, data is shared via virtual data centers from the customers and the organization [2].




Fig. 1: Fee Collection System

Cloud computing has evolved as a popular and universal paradigm for service-oriented computing where computing infrastructure and solutions are delivered as a service. The cloud has revolutionized the abstraction and use of computing infrastructure through its features (e.g., self-service on-demand, broad network access, resource pooling, etc.), making cloud computing desirable [3]. However, security is the biggest challenge, and concerns regarding cloud computing continue to arise as we witness an increasing number of new developments in cloud computing platforms. In the post-COVID-19 world, it is clear that more people and businesses are adopting cloud services, software, and infrastructure, as they can be accessed anytime, and from anywhere. To handle security risks, several research works and developments, such as in [4,5], have been proposed. Nonetheless, there are still more opportunities for new techniques to make the cloud more secure, as shown in fig 1. Most of the existing techniques for securing the cloud do not focus on the new types of security risks that might face the cloud computing infrastructure. Hence, they cannot detect attacks or vulnerabilities that might come from the cloud service provider's side or the consumer's side.

## 2. LITERATURE SURVEY

Fahad Alqahtani, et al. [6] proposed the CloudMonitor framework to strengthen cloud security by preventing the unauthorized exfiltration and extrusion of sensitive information stored in cloud environments. The framework was designed to provide enhanced Information Flow Tracking (IFT), allowing Cloud Service Consumers (CSCs) to monitor, analyze, and control how their data

International Journal of
AI EBIOMEDICINE INNOVATIONS
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0507 www.zesterapublications.com Original Research Paper

is accessed, transferred, and processed by third-party cloud services. Both centralized and dynamic IFT mechanisms were implemented to improve transparency and enable real-time detection of suspicious data movements. Experimental evaluation demonstrated that the framework enhances visibility into cloud data transfers while reducing the risk of data leakage, unauthorized information disclosure, and insider attacks. Hongyi Hao [7] presented a comprehensive review of modern cloud data security technologies, including encryption techniques, access control mechanisms, privacy-preserving computation, Zero Trust Architecture, and threat intelligence systems. The study evaluated these technologies using practical case studies and concluded that no single security mechanism can provide complete protection against evolving cyber threats. Instead, integrating multiple security approaches creates a stronger defense by improving confidentiality, integrity, privacy, and resilience against sophisticated attacks. Liang Yan, et al. [8] proposed a blockchain-enabled cloud access control framework based on Attribute-Based Searchable Encryption (ABSE) to provide secure and fine-grained data access in cloud environments. The proposed scheme incorporated proxy encryption and proxy decryption to reduce computational overhead while supporting attribute revocation and policy hiding. Encrypted files were securely stored using the InterPlanetary File System (IPFS), whereas metadata ciphertext was maintained on the blockchain to guarantee data confidentiality, integrity, traceability, and tamper resistance. Swatisipra Das, et al. [9] conducted a comprehensive analysis of cloud security challenges by categorizing existing threats according to major security requirements such as confidentiality, integrity, availability, authenticity, and privacy. The study systematically investigated blockchain-based solutions for cloud security, focusing on identity management, access control, secure authentication, and data integrity verification. The findings demonstrated that blockchain technologies provide decentralized trust, improved transparency, and enhanced resistance against unauthorized access and data manipulation in cloud computing environments.

Chauhan M., et al. [10] presented an extensive comparative study of widely adopted cloud security frameworks used to secure modern cloud infrastructures. The research examined major frameworks including Control Objectives for Information and Related Technologies 5 (COBIT 5), National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO), Cloud Security Alliance (CSA) STAR, and the Amazon Web Services (AWS) Well-Architected Framework. Each framework was evaluated based on its security objectives, implementation methodology, strengths, limitations, deployment requirements, and practical applicability. The study also analyzed common cloud security issues and emphasized the importance of selecting appropriate security governance models for protecting cloud services. Mustafa Al Lail, et al. [11] proposed an optimized cloud-based implementation of the Generalized Spatio-Temporal Role-Based Access Control (GSTRBAC) model for Location-Based Services (LBS). The proposed framework granted user access according to authenticated identities, geographical locations, temporal constraints, and assigned permissions, thereby providing fine-grained access control suitable for cloud-enabled LBS applications. Experimental analysis demonstrated that the optimized GSTRBAC implementation improves authorization accuracy while strengthening the protection of location-sensitive information stored in cloud environments. Yunliang Li, et al. [12] introduced the Role-Based Access Control for Inter-System Cross-Domain (RBAC-IC) model to address access management challenges within multi-domain cloud computing environments. The proposed framework separated user roles into abstract and specific categories

International Journal of
AI EBIOMEDICINE INNOVATIONS
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0507 www.zesterapublications.com Original Research Paper

while resolving issues related to role naming conflicts, platform-domain isolation, inter-domain authorization, and secure cross-domain resource sharing. The model enabled fine-grained access control, improved interoperability among multiple cloud domains, and simplified secure permission management across distributed enterprise systems.

Shahnawaz Ahmad, et al. [13] proposed a Hybrid Cryptographic Approach for Key Management Systems (HCA-KMS) in cloud computing by integrating Advanced Encryption Standard (AES) with Elliptic Curve Cryptography (ECC). The proposed scheme enhanced authenticated encryption while improving confidentiality, integrity, resource utilization, storage efficiency, and computational performance. Comparative analysis demonstrated that HCA-KMS achieved efficient encryption and decryption with reduced computational complexity, making it suitable for secure cloud-based data protection. Regueiro, et al. [14] proposed a blockchain-based audit trail framework to strengthen accountability, transparency, and integrity in cloud computing environments. The architecture leveraged blockchain technology to generate secure, tamper-resistant, and verifiable audit logs capable of tracking every operation performed on cloud resources. The proposed prototype demonstrated that decentralized audit mechanisms effectively eliminate vulnerabilities associated with conventional logging systems while providing reliable forensic evidence, secure event monitoring, and trustworthy audit management for cloud infrastructures.

## 3. PROPOSED SYSTEM

This research describes the implementation of the secure web-based management system developed using the Flask framework in Python. Flask is used to handle Hypertext Transfer Protocol (HTTP) requests, session management, role-based authentication, and integration of backend modules. The system implements user authentication using Flask-Login and password security using Werkzeug's hashing algorithms. For data storage, TinyDB is used to manage users, files, complaints, payments, audit logs, and maintenance records. To ensure data confidentiality, a hybrid encryption approach is implemented, combining RSA public key encryption and AES symmetric encryption (AES-GCM mode) for secure file storage and message exchange shown in Fig. 2. RSA is used for secure key distribution, while AES provides efficient and secure encryption of large files. The modular architecture using Flask Blueprints improves maintainability, scalability, and separation of concerns across different user roles such as admin, database manager, and user.

International Journal of
AI EBIOMEDICINE INNOVATIONS
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0507 www.zesterapublications.com Original Research Paper

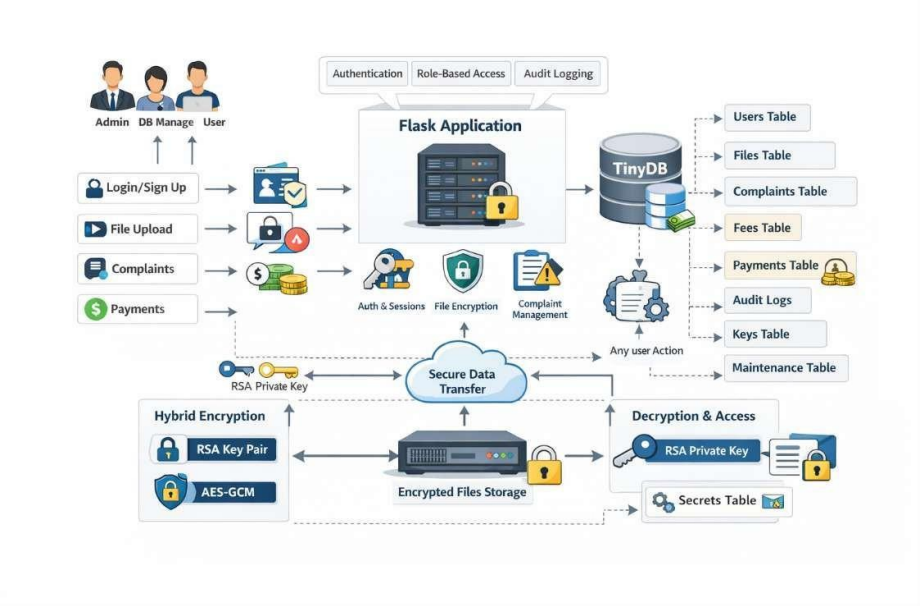



Fig. 2: Proposed System Architecture of Cloud Database Maintenance Fee Collection

**User Authentication and Role Validation:** The system begins when the Admin, DB Manager, or User logs in through the web interface. Flask validates credentials and establishes a secure session using role-based access control. Only authenticated users are allowed to access system services.

**Request Processing via Flask Application:** All user actions such as file upload, complaints, or payments are routed to the Flask application. Flask acts as the central controller, managing HTTP requests, sessions, and permissions. Role restrictions are enforced before processing any request.

**Secure File Encryption and Data Protection:** When files or sensitive data are submitted, the system applies hybrid encryption. AES-GCM encrypts the actual file content, while RSA encryption secures the AES key. This ensures confidentiality and integrity of stored data.

**Encrypted Storage and Database Management:** Encrypted files are stored in the server file system, while metadata is maintained in TinyDB tables. TinyDB manages users, files, complaints, fees, payments, audit logs, keys, and maintenance records securely.

**Secure Data Access and Decryption:** During file access, the RSA private key is used to decrypt the AES key. The AES-GCM algorithm then decrypts the file only for authorized users. Integrity verification ensures that tampered data is rejected.

**Audit Logging and System Monitoring:** Every critical operation such as login, file access, and payments is recorded in audit logs. This provides accountability, traceability, and supports system monitoring and compliance requirements.

## 4. RESULT ANALYSIS

International Journal of
AI EBIOMEDICINE INNOVATIONS
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0507 www.zesterapublications.com Original Research Paper

Fig. 3 depicts the User Management Screen which facilitates the administration of registered users in the system. It displays user-related information including roles, contact details, and registration data. The interface supports role assignment and controlled modification of user privileges. It reflects the enforcement of role-based access control within the cloud environment.

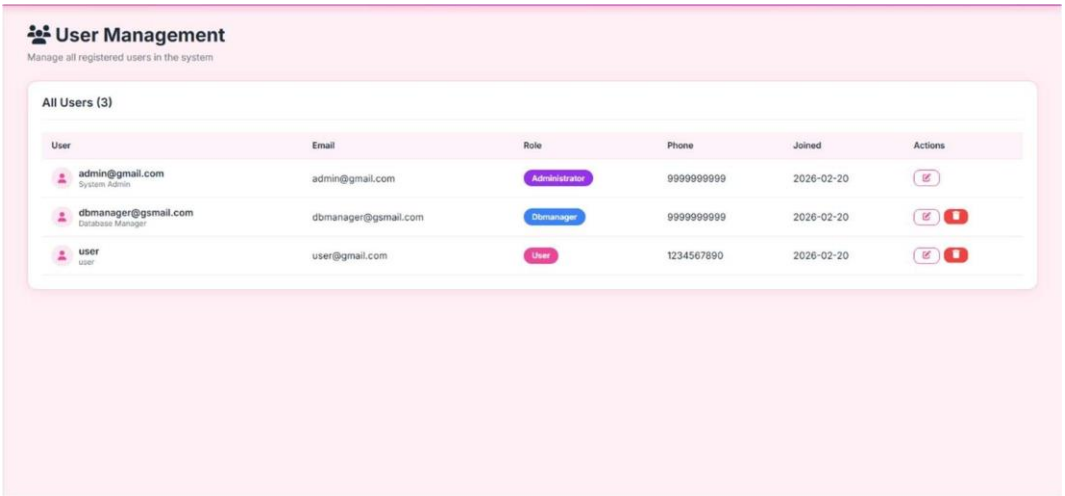



Fig. 3: User Management Screen

Fig. 4 illustrates the Fee Configuration Screen that enables the creation and management of maintenance fees. It demonstrates how administrators define fee details, amounts, descriptions, and due dates within the system. The screen also provides visibility into active fee records for monitoring financial activities. It supports systematic tracking of payment-related configurations.

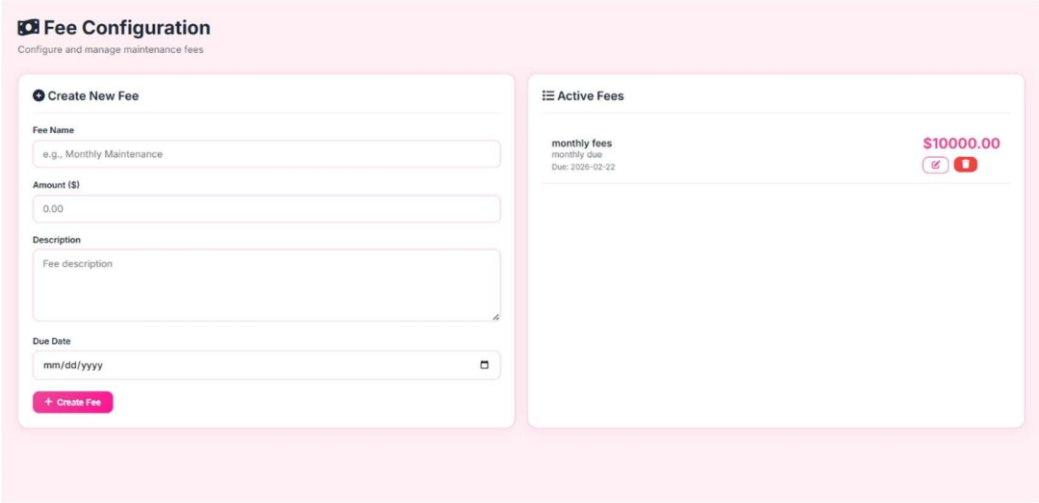



Fig. 4: Fee Configuration Screen

Fig. 5 depicts the Complaint Review Screen which manages user-submitted issues and service requests. It presents complaint details such as subject, category, priority, and resolution status. The interface supports review and response mechanisms for administrative handling. It enhances communication transparency between users and system authorities.

International Journal of
AI EBIOMEDICINE INNOVATIONS
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0507 www.zesterapublications.com Original Research Paper

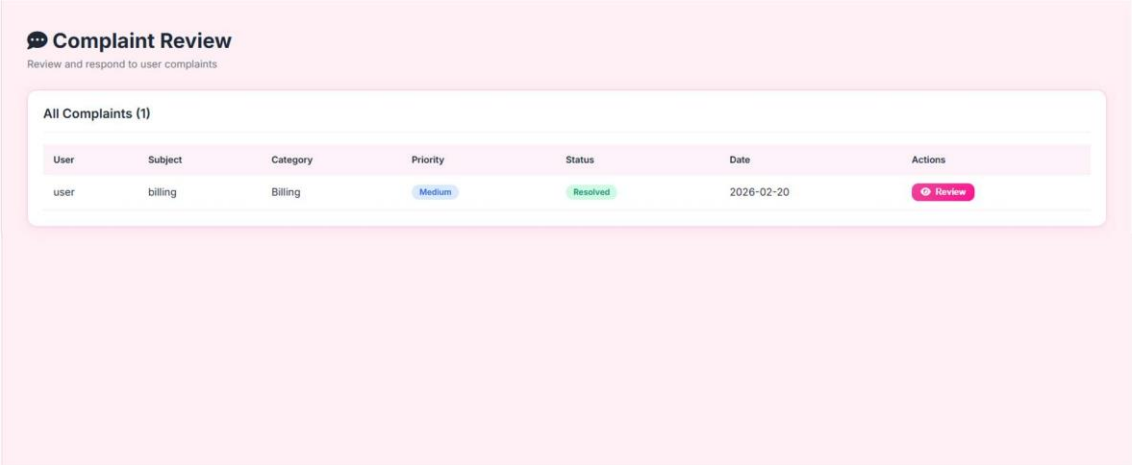



Fig.5: Complaint Review Screen

Fig. 6 depicts the Database Monitoring Screen designed to track database performance and system health metrics. It displays storage utilization, file statistics, active users, and transaction information to support real-time monitoring. The interface provides insights into database connectivity and encryption configuration to ensure operational transparency. It also reflects secure cloud transfer capabilities that support protected data movement.

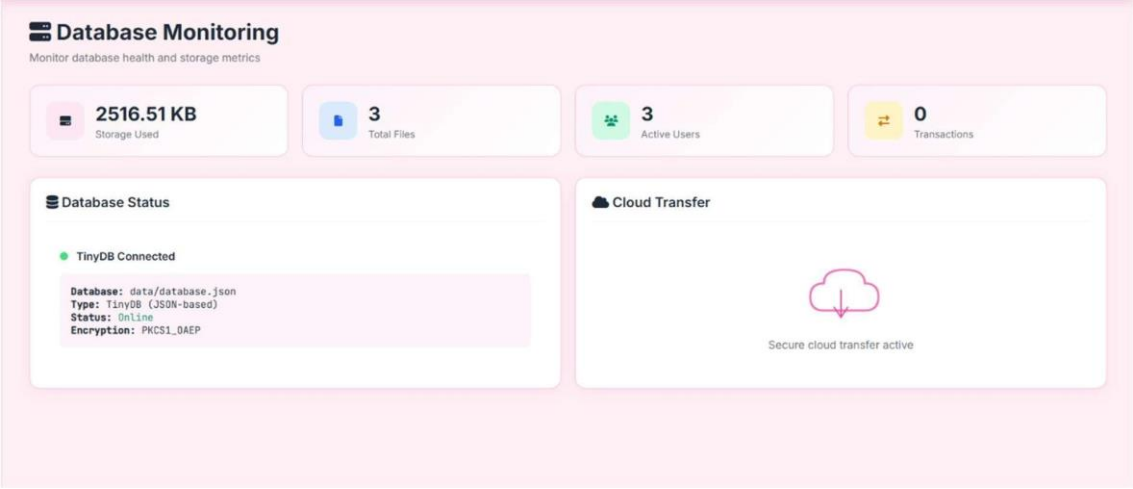



Fig. 6: Database Monitoring Screen

Fig. 7 depicts the Maintenance Scheduling Screen used for organizing and managing database maintenance activities. It allows administrators or managers to define maintenance tasks, descriptions, and scheduled timelines. The interface displays upcoming maintenance operations to support planning and system continuity. It reflects the structured workflow for handling system updates, backups, and operational improvements.

International Journal of
AI EBIOMEDICINE INNOVATIONS
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0507 www.zesterapublications.com Original Research Paper

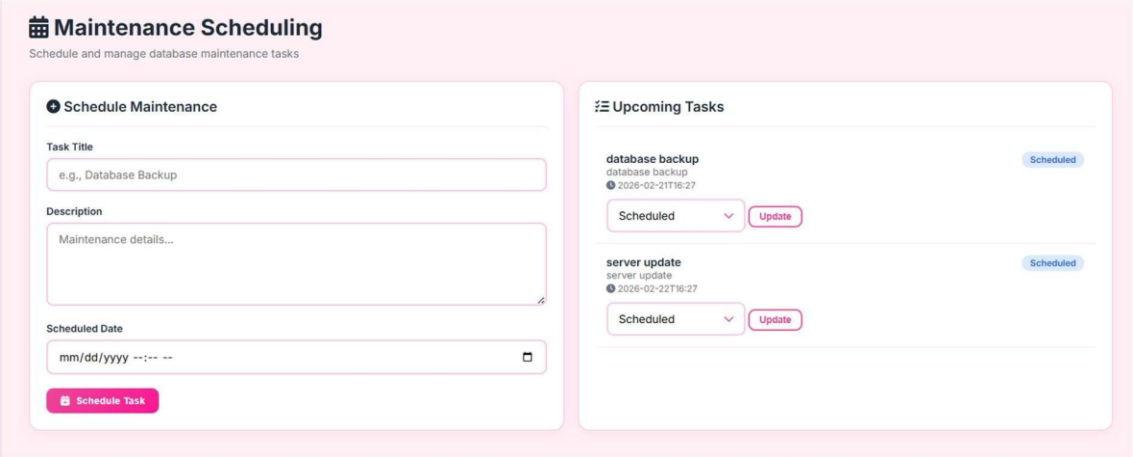



Fig. 7: Maintenance Scheduling Screen

Fig. 8 illustrates the Fee Payment Screen designed for secure handling of maintenance fee transactions. It displays available fees along with payment history records to ensure financial transparency. The interface supports secure payment processing within the protected system environment. It enables users to track completed transactions and manage payment responsibilities effectively.

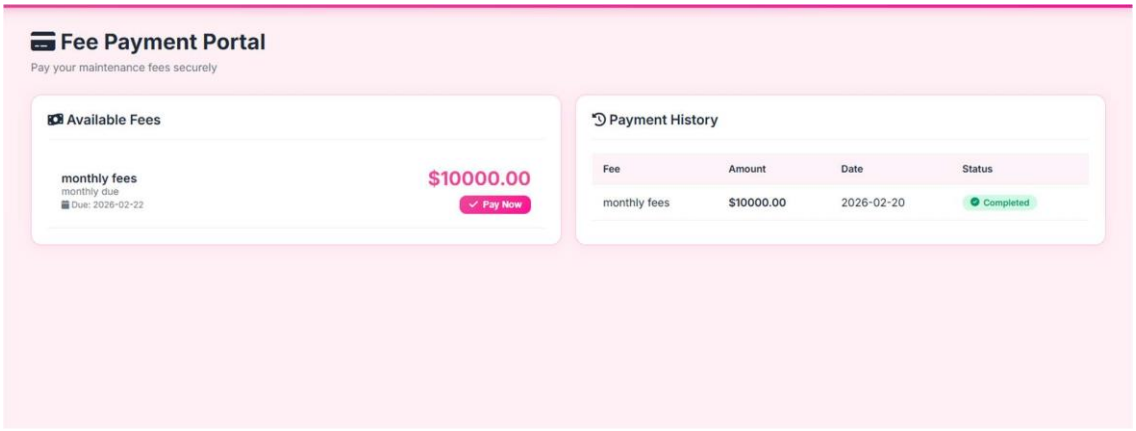



Fig. 8: Fee Payment Screen

## 5. CONCLUSION

This research effectively addresses the critical challenges associated with traditional cloud-based database management systems, particularly in terms of security, access control, and operational transparency. By integrating RBAC with a hybrid cryptographic approach using RSA and AES-GCM, the system ensures strong data confidentiality, integrity, and controlled accessibility across different user roles. The use of TinyDB as a lightweight NoSQL database demonstrates that efficient and scalable data management can be achieved without relying on complex and resource-intensive database infrastructures. Furthermore, the incorporation of secure complaint handling, maintenance fee tracking, and detailed audit logging enhances accountability and provides a transparent operational framework. the system significantly reduces the risks of unauthorized

International Journal of
AI EBIOMEDICINE INNOVATIONS
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0507 www.zesterapublications.com Original Research Paper

access, improves monitoring capabilities, and streamlines administrative processes. The implementation using Flask enables flexibility and ease of deployment, making the solution practical for real-world organizational environments.

## REFERENCES

[1] Elsherbiny, S.; Eldaydamony, E.; Alrahmawy, M.; Reyad, A.E. An extended Intelligent Water Drops algorithm for workflow scheduling in a cloud computing environment. Egypt. Inf. J. 2018, 19, 33–55

[2] Hanen, J.; Kechaou, Z.; Ben Ayed, M. An enhanced healthcare system in a mobile cloud computing environment. Vietnam J. Comput. Sci. 2016, 3, 267–277.

[3] Mell, P.; Grance, T. The NIST Definition of Cloud Computing; Nation-al Institute of Standards and Technology: Gaithersburg, MD, USA, 2011.

[4] Hatwar, S.V.; Chavan, R. Cloud Computing Security Aspects, Vulnerabilities and Countermeasures. Int. J. Comput. Appl. 2015, 119, 46–53.

[5] Dinh, P.T.; Park, M. Dynamic Economic-Denial-of-Sustainability (EDoS) Detection in SDN-based Cloud. Proceedings of the 2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC), Paris, France, 20–23 April 2020.

[6] Alqahtani, F.; Almutairi, M.; Sheldon, F.T. Cloud Security Using Fine-Grained Efficient Information Flow Tracking. Future Internet 2024, 16, 110. https://doi.org/10.3390/fi16040110

[7] Hao, H. Data security strategies and technologies for robust cloud computing. Discov Appl Sci 8, 91 (2026). https://doi.org/10.1007/s42452-025-08091-x

[8] Yan, L., Ge, L., Wang, Z. et al. Access control scheme based on blockchain and attribute-based searchable encryption in cloud environment. J Cloud Comp 12, 61 (2023). https://doi.org/10.1186/s13677-023-00444-4

[9] Das, S.; Priyadarshini, R.; Mishra, M.; Barik, R.K. Leveraging Towards Access Control, Identity Management, and Data Integrity Verification Mechanisms in Blockchain-Assisted Cloud Environments: A Comparative Study. J. Cybersecur. Priv. 2024, 4, 1018-1043. https://doi.org/10.3390/jcp4040047

[10] Chauhan, M.; Shiaeles, S. An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions. Network 2023, 3, 422-450. https://doi.org/10.3390/network3030018

[11] Al Lail, M.; Moncivais, M.; Benton, R.; Perez, A.J. Cloud-Based Access Control Including Time and Location. Electronics 2024, 13, 2812. https://doi.org/10.3390/electronics13142812

International Journal of
AI EBIOMEDICINE INNOVATIONS
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0507 www.zesterapublications.com Original Research Paper

[12] 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

[13] Ahmad, S., Mehfuz, S. & Beg, J. Hybrid cryptographic approach to enhance the mode of key management system in cloud environment. J Supercomput 79, 7377–7413 (2023). https://doi.org/10.1007/s11227-022-04964-9

[14] Regueiro, C.; Seco, I.; Gutiérrez-Agüero, I.; Urquizu, B.; Mansell, J. A Blockchain-Based Audit Trail Mechanism: Design and Implementation. Algorithms 2021, 14, 341. https://doi.org/10.3390/a14120341