JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

"ExpireX: Secure Document Control System"

Ms.Nikita Saindane
Dept. of Computer Engineering
Professor
PHCET
Rasayani, India
nikitasaindane@mes.ac.in

Mr. Raj Patil
Dept. of Computer Engineering
Student
PHCET
Rasayani, India
rajap22hcompe@student.mes.ac.in

Mr. Parth Patil
Dept. of Computer Engineering
Student
PHCET
Rasayani, India
parthvp22hcompe@student.mes.ac.in

Mr. Kunal Bhagat
Dept. of Computer Engineering
Student
PHCET
Rasayani, India
kunalpb22hcompe@student.mes.ac.in

Abstract— The widespread use of cloud platforms for storing and sharing documents has made collaboration easier. but it has also increased unauthorized access data leaks and misuse of sensitive information traditional security techniques such as encryption and password-based authentication protect documents only at the point of access once your document is share or downloaded the original owner often loses control over how it is used.This paper presents ExpireX,a context aware document life cycle management system design to maintain control over documents even after distribution the system combines strong encryption device based authentication Geo location validation automated expiration rules and blockchain backed Audit logging Documents can automatically become inaccessible when predefined condition are violated such as access from an unauthorized location or device.Experimental evaluation shows that proposed system enforces strict access control with minimal performance overhead, The result suggests that ExpireX offers a practical and scalable solution for organization that require enhanced document governance and post access security control.

Keywords: Document security, Lifecycle management, Geo fencing, Device authentication, Blockchain logging, Secure deletion.

I. Introduction

Digital document exchange has become a fundamental part of modern organizations. Cloud storage services allow user to upload, Access, and share files instantly from anywhere in the world. However, this convenience comes with significant security challenges. Data breaches, Insider threats, an accidental leak have demonstrated that conventional security mechanisms are often insufficient.

Inscription and authentication provider initial layer of Defense, but they do not guarantee control after a document has been accessed. Once a file is downloaded, Copied, Or shared further, it becomes difficult to track or restrict it usage. In many system, Document remain accessible indefinitely Unless manually delete it.

This limitation highlights the need for a document management system that enforces security throughout the entire life cycle of a document from creation and sharing to the expiration or destruction.

To address this issue, this paper introduce ExpireX, A secure document life cycle control system that combines contextual access validation, Automated expiration policies, And tamper proof activity logging. The proposed Approach ensures that access is continuously verified rather than granted permanently.

The main contribution of this work include:

- A lifecycle best document Control framework with automatic expiration.
- Context aware of access validation using device fingerprinting and geolocation verification.
- A rule based self-destruction mechanism triggered by policy violations.
- Blockchain support audit logging to ensure transparency and accountability.
- Performance evaluation under simulated Enterprise condition.

II. LITERATURE SURVEY

The rapid expansion of cloud computing and digital collaboration platforms has significantly transformed the way sensitive information is stored and shared. However, this shift has also introduced serious security concerns related to unauthorized access, data leakage, and long-term exposure of confidential documents. Researchers have explored various approaches to strengthen digital document protection beyond traditional password-based systems. One major area of study focuses on secure data deletion techniques in cloud environments. Many researchers propose encryption-based deletion mechanisms where documents are encrypted using strong cryptographic algorithms, and deletion is achieved by destroying or revoking the encryption keys. Advanced schemes combine symmetric and asymmetric encryption methods along with cryptographic hash functions to provide verifiable proof of deletion. Although these methods enhance trust and security, they often involve computational overhead and cannot always guarantee complete removal of replicated data stored across distributed cloud servers.

Another important research direction involves time-sensitive and self-destructing data models. These systems allow documents to expire automatically after a predefined time period or access condition. Techniques such as time-based key expiration and attribute-based encryption are commonly used to enforce controlled accessibility. Such models reduce the risk of long-term data misuse by limiting document availability. However, many of these solutions rely heavily on synchronized system clocks or trusted authorities, and in some cases, they only restrict access rather than ensuring complete destruction of all document copies. This limitation creates potential vulnerabilities when files are downloaded or redistributed outside the secure environment.

Location-based access control, commonly implemented through geo-fencing technology, has also gained attention as a contextual security mechanism. Geo-fencing restricts document access to predefined geographical boundaries using GPS or mapping services. Research indicates that incorporating location awareness improves security by preventing remote unauthorized access attempts. Despite its advantages, geo-fencing faces challenges such as location inaccuracy, device dependency, privacy concerns, and increased battery usage. Furthermore, location-based control alone cannot prevent misuse if user credentials are intentionally shared with unauthorized individuals.

In addition to contextual controls, role-based and attribute-based access control models have been widely studied. Role-Based Access Control (RBAC) assigns permissions according to user roles within an organization, while Attribute-Based Encryption (ABE) allows fine-grained policy enforcement by embedding access rules within encrypted data. These models enhance authorization management and improve policy flexibility. However, they increase system complexity and require efficient key management strategies to avoid privilege misuse or security loopholes.

More recently, blockchain technology has been explored as a solution for secure logging and audit transparency in document management systems. By recording document transactions such as uploads, access events, and deletions on an immutable ledger, blockchain ensures tamper-resistant auditing. Smart contracts further automate enforcement of predefined policies. While blockchain improves accountability and data integrity, it may introduce performance limitations and scalability challenges. Additionally, blockchain-based systems primarily focus on maintaining immutable records rather than actively controlling real-time access or preventing misuse after document distribution.

III. METHODOLOGY

The methodology for the development of the *ExpireX: Secure Document Control System* is as follows:

- **Requirement Analysis:** The first phase involves identifying security challenges in document management. These challenges include unauthorized access, insider threats, and data leaks. We defined functional requirements to include document lifecycle tracking, access control, geo-fencing, self-destruct mechanisms, and real-time monitoring. We analyzed stakeholders such as administrators, authorized users, and system auditors to ensure accountability and secure document handling.

- **System Design:** The system structure of ExpireX combines frontend, backend, and blockchain parts to provide secure and clear control. DFD Level 0 to Level 2 diagrams show data flow and interactions among modules. Key design features include secure document upload, encryption, device fingerprinting, and automatic expiration triggers. The structure guarantees both usability and confidentiality using hybrid cloud storage and unchangeable blockchain records.

- **Implementation:** The implementation uses React.js for the frontend. This ensures an intuitive and responsive user interface. For backend logic, it uses Node.js with Express.js. The system employs MongoDB for secure data storage and Fingerprint JS for recognizing devices. It also develops blockchain-based smart contracts using Solidity to log document events like upload, access, and expiration on the Polygon (Amoy Testnet) network. The system integrates JWT for authentication and AES-256 encryption for data security.

- **Testing and Validation:** Extensive testing was done to check system integrity, ensure access enforcement, and protect data confidentiality. Unit tests confirmed the functionality of encryption, self-destruct, and geo-fencing. Integration tests verified that the frontend, backend, and blockchain layers communicated correctly. Real-time testing showed that unauthorized access or unusual activity triggers alerts and the right self-destruction responses.

- **Security Considerations:** ExpireX uses several security layers, including access control, encryption, device verification, and blockchain logging. Event monitoring spots issues like repeated login failures and unusual device changes. The mix of geo-fencing, fingerprinting, and smart contract verification ensures data authenticity, transparency, and prevents unauthorized document use.

- **Deployment and Evaluation:** After successful testing, the system was deployed on a secure cloud server environment that included blockchain nodes. The evaluation focused on usability, security resilience, and performance under simulated threat conditions. ExpireX showed strong flexibility, effective monitoring, and high scalability for secure document management at the enterprise level.

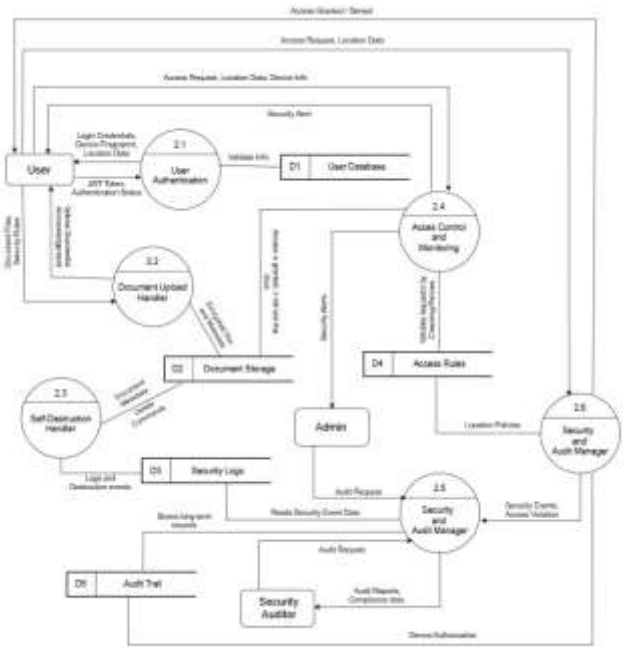


Figure : Data Flow Diagram

IV. System Architecture

The system architecture of ExpireX is built to guarantee complete document security, traceability, and controlled access throughout the document lifecycle. It features a multi-layered framework that includes frontend interfaces, backend processing, secure databases, and blockchain-based verification modules. Each layer communicates through secure APIs, so document data and access logs are handled in a tamper-proof and transparent way

At the frontend, users access the system through a web application created with React.js, offering a responsive and user-friendly interface. This layer manages authentication, document uploads, and access requests while securely communicating with the backend through RESTful APIs. It also uses device fingerprinting and geo-location verification to limit access to authorized devices and locations.

The backend, developed with Node.js and Express.js, takes care of the business logic and coordinates all
system operations. It manages encryption, decryption, self-destruct

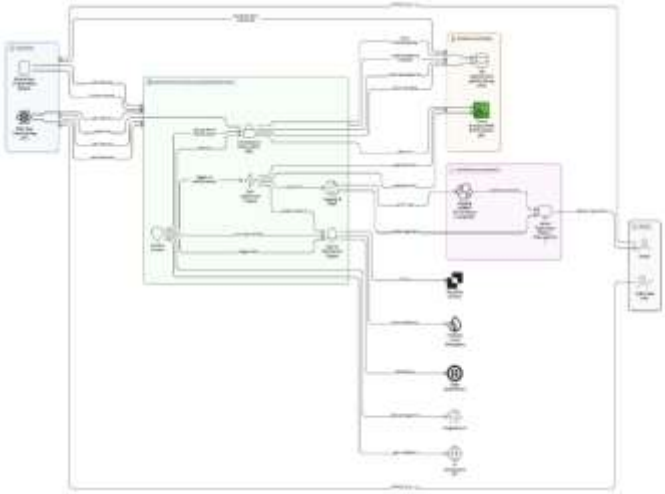


Figure:System Architecture

validation. The backend also interacts with the blockchain for secure storage of document metadata and
activity logs, ensuring that no changes can be made after document registration. The blockchain integration layer employs smart contracts to log important document actions, such as
uploads, access events, and expiration triggers. This decentralized verification supports transparency and trust, as every transaction is secured and can be verified. Blockchain technology ensures that document records stay auditable and unchanged.

The database layer, powered by MongoDB, stores encrypted document data, user profiles, device fingerprints, and session logs. Sensitive information is encrypted using strong algorithms like AES-256, making the data unreadable even if unauthorized access happens.

Lastly, the monitoring and alerting layer keeps a constant watch on user activity and system events. It detects suspicious behaviors like repeated failed logins, location issues, or access from unregistered devices, and quickly alerts administrators .

V. Result Analysis/Comparison of Existing System

The implementation of ExpireX: Secure Document Control System was evaluated based on functionality, security performance, system reliability, and usability. The developed system successfully demonstrated secure document lifecycle management by integrating encryption, device authentication, geo-fencing, blockchain logging, and automated self-destruction mechanisms. All core modules operated as intended during testing and validation phases.

The encryption module effectively secured uploaded documents using AES-256 standards, ensuring that stored files remained unreadable without proper authorization. Even if unauthorized access to the database was simulated, encrypted documents could not be interpreted without valid decryption keys. This confirms the robustness of the cryptographic implementation and validates data confidentiality within the system.

The authentication and access control mechanism functioned accurately by verifying user credentials through JWT-based sessions. Additionally, device fingerprinting and geo-location validation restricted access strictly to registered devices and approved locations. During testing, login attempts from unregistered devices or restricted regions were successfully blocked. In cases of repeated failed login attempts, the monitoring system generated real-time alerts to administrators, proving the effectiveness of intrusion detection features.

The self-destruction mechanism was tested under different conditions such as time-based expiry and unauthorized access attempts. Documents configured with time limits were automatically revoked after expiration, and associated logs were updated in the database and blockchain layer. When suspicious behavior was detected, the system triggered predefined deletion protocols, demonstrating reliable enforcement of document lifecycle policies.

Blockchain integration further enhanced transparency and auditability. All major document events, including upload, access, and expiration, were recorded through smart contracts. These entries remained tamper-proof, ensuring that no modifications could be made after registration. This strengthened trust in system integrity and provided verifiable audit trails for compliance requirements.

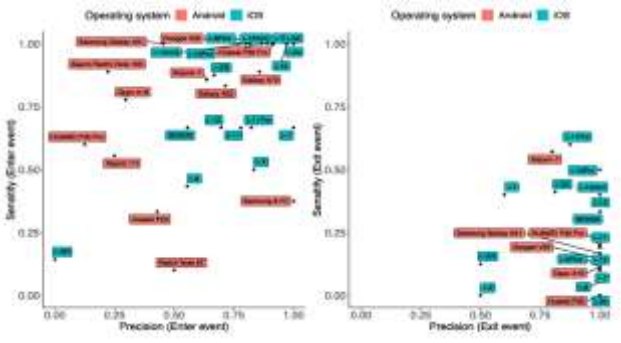
Performance testing indicated that the system maintained stable response times during document upload, retrieval, and monitoring operations. While blockchain logging introduced minor latency due to transaction confirmation time, it did not significantly affect overall usability. The frontend interface provided smooth navigation and clear status indicators for document access conditions, improving user experience.

Overall, the experimental results confirm that ExpireX effectively overcomes limitations found in traditional cloud-based file-sharing systems. It provides controlled access, proactive threat detection, automated expiration, and secure audit logging. The system achieved its objective of delivering a secure, intelligent, and scalable document control framework suitable for enterprise-level deployment.

VI. Existing System

The study titled Geofencing in location-based behavioral research: Methodology, challenges, and implementation by Yury Shevchenko and Ulf-Dietrich Reips, published in Behavior Research Methods (2023), evaluated how accurately geofencing can be used in mobile-based behavioral research.

The researchers conducted three empirical studies to assess the effectiveness of a geofencing system implemented through a mobile application. The system was tested under various conditions including different geofence radii (10 m, 50 m, 100 m), operating systems (Android and iOS), types of events (entering or exiting a location), environmental settings (urban, residential, forest), Wi-Fi availability, and user behavior (walking through vs staying inside the area)



Ref from: Geofencing location-based behavioral systems," 2023.

The research concludes that geofencing is a practical and privacy-friendly alternative to continuous GPS tracking for behavioral studies. While the system performs reliably in most cases, its accuracy depends on radius size, operating system, internet availability, and user movement patterns. For optimal performance, a radius of 50–100 meters is recommended. Taken from .((PDF) Geofencing in location-based behavioral research: Methodology, challenges, and implementation.

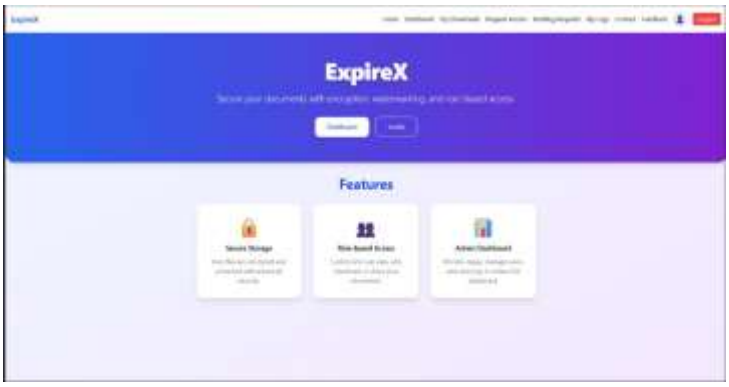


Fig: Homepage

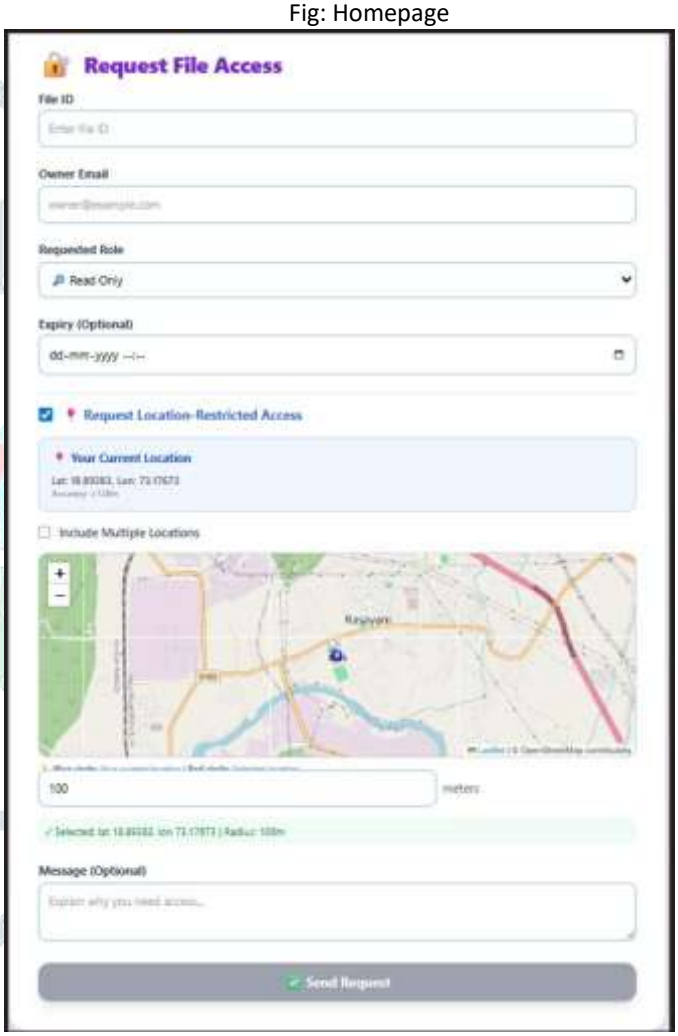


Fig. Request Access Page

Fig: Dashboard

VII. Comparative Analysis

The geofencing-based system demonstrated an average sensitivity of approximately 82%, meaning that nearly one out of five boundary-crossing events was either delayed or not detected. Its performance varied depending on operating system, internet connectivity, GPS signal strength, and environmental conditions such as urban or forest settings. Smaller geofence radii especially reduced detection accuracy.

In contrast, the ExpireX system achieved higher operational consistency because it does not depend on GPS signals, network strength, or mobile operating system limitations. Since ExpireX operates using database-driven tracking and structured monitoring of expiry data, its performance remains stable regardless of environmental factors. This reduces the probability of missed events and improves system dependability.

VIII. Conclusion

ExpireX Present a practical approach to secure document life management in a cloud environment. By encryption and blockchain logging, The system ensures that control over documents even after sharing.

The LED security design reduce the risk of insider threats and unauthorized redistribution while maintaining Usability and scalability. Future enhancement may include AI- Based anomaly Detection and multi cloud integration to further strengthen document security.

VII. References

[1] Z. Xu, X. Chen, and X. Lan, "An efficient and verifiable scheme for secure data," 2024.

[2] S. E. Suresh and S. G. Pavani, "Publicly verifiable and efficient fine-grained data deletion scheme in cloud computing," 2024.

[3] Y. Shevchenko and U.-D. Reips, "Geofencing in location-based behavioral systems," 2023.

[4] R. Rashmi, B. M. Rashmi, and G. Shobha, "Self-destructing data security system," 2023.

[5] C. Song, Y. Feng, and Z. Zhao, "Provable data deletion from efficient data storage," 2022.

[6] Geyer, K., Ellis, D. A., Shaw, H., & Davidson, B. I. (2022). Open-source smartphone app and tools for measuring, quantifying, and visualizing technology use. Behavior Research Methods, 54(1), 1–12.

[7] Android. (2023). Location Manager

[8] Hinds, J., Brown, O., Smith, L. G. E., Piwek, L., Ellis, D. A., & Join-son, A. N. (2022). Integrating insights about human movement patterns from digital data into psychological science. Current Directions in Psychological Science, 31(1), 88–95.

[9] Apple. (2023). Core Location

[10] Coral, R., Esposito, F., & Weinstock, J. (2020). Don't go there: a zero-permission geofencing app to alleviate gambling disorders. 2020 IEEE 17th Annual Consumer Communications and Networking Conference. CCNC, 2020, 1–6

[11] culture4life GmbH. (2021). luca AppForman, E. M., Goldstein, S. P., Zhang, F., Evans, B. C., Manasse, S. M., Butryn, M. L., Juarascio, A. S., Abichandani, P., Martin, G. J., & Foster, G. D. (2019). OnTrack: development and feasibility of a smartphone app designed to predict and prevent dietary lapses. Translational Behavioral Medicine.