International Journal of Combined Research & Development (IJCRD)
eISSN:2321-225X; pISSN:2321-2241 Volume: 14; Issue: 8; August- 2025

SAFEGUARDING MULTI-USER DATA UPDATES WITH ADVANCED ENCRYPTION TECHNIQUES

Chandan Kumar Mahanta
PG, Student
Dept. of MCA
The Oxford College of Engineering,
Bommanahalli, Bengaluru- 560068
chandankumarmahantamca2025@gmail.com

Sowmya J
Assistant Professor
Dept. of MCA
The Oxford College of Engineering,
Bommanahalli, Bengaluru- 560068
sowmyaj@theoxford.edu

ABSTRACT

In today's digital world, managing and securing shared data across multiple users has become a critical requirement. Traditional systems often fail to provide strong protection during data updates, making sensitive information vulnerable to unauthorized access or tampering. This study introduces a secure framework designed to safeguard multi-user data updates by integrating advanced encryption techniques with layered authentication mechanisms. The proposed system ensures that every user request is validated through trustee-based verification and centralized administration, reducing risks of misuse and unauthorized modifications. Strong cryptographic methods are applied to protect the integrity and confidentiality of data, while role-based access control defines clear responsibilities for users, trustees, and administrators. To enhance reliability, the system also incorporates recovery options and monitoring features, creating a balance between security and usability. Experimental evaluation shows that the framework achieves improved protection, scalability, and adaptability without compromising efficiency. The results highlight its effectiveness in environments where multiple stakeholders access and update shared records, such as enterprise systems, educational institutions, and government organizations.

KEYWORDS: *Data security, multi-user updates, encryption, authentication, trustee verification, access control*

INTRODUCTION

The expansion of online services and collaborative platforms has increased the demand for secure handling of shared data among multiple users. Every update performed in such environments carries the risk of unauthorized modification, accidental data

loss, or malicious intrusion. Traditional methods often rely on simple password-based authentication or limited encryption, which cannot effectively safeguard critical information in large-scale multi-user settings. Security breaches and unauthorized access not only compromise sensitive data but also weaken trust in digital systems.

To overcome these limitations, modern frameworks must combine robust encryption algorithms with multi-level access control and verification mechanisms. In particular, trustee-based validation and centralized administration can ensure that only legitimate requests are processed, while unauthorized actions are systematically blocked. This paper introduces a framework that integrates advanced encryption with role-based authentication to safeguard multi-user updates, ensuring both security and efficiency in collaborative digital environments.

LITERATURE SURVEY

Securing data updates in multi-user environments has been a significant research focus for decades. Early systems primarily depended on basic cryptographic methods and password authentication. While these techniques provided minimal protection, they often lacked scalability and robustness when multiple users attempted to update shared records simultaneously. This limitation created opportunities for unauthorized access, data manipulation, and reduced system reliability.

Researchers soon introduced role-based access control (RBAC) models, where user roles and permissions were clearly defined. Though effective in structured organizations, RBAC alone was insufficient against advanced attacks and insider threats. To improve protection, identity-based encryption and public key infrastructures were proposed, offering stronger confidentiality and secure key management. Shamir's and Boneh's cryptographic schemes are frequently cited as pioneering work in this domain, demonstrating the potential of encryption in safeguarding sensitive data exchanges.

Recent studies emphasize integrating encryption with layered security features such as trustee-based verification and centralized monitoring. Trustee verification introduces an additional approval stage, ensuring that updates are validated before being committed. This prevents malicious alterations and enhances accountability. Centralized monitoring allows administrators to oversee activities, providing transparency and quick responses to suspicious actions.

The literature suggests that while cryptographic foundations remain vital, combining encryption with multi-level verification, monitoring, and administrative control results in a more comprehensive solution. Building on these insights, the present work proposes a system that addresses both security and usability in safeguarding multi-user data updates.

EXISTING WORK

Existing approaches to securing multi-user data updates have relied on a variety of mechanisms ranging from traditional encryption to structured access control systems. Early solutions employed symmetric and asymmetric encryption techniques to protect the confidentiality of shared data. While these methods ensured basic security, they often lacked mechanisms to validate user intent during updates, leaving opportunities for unauthorized modifications.

To address these challenges, role-based access control (RBAC) and discretionary access control (DAC) models were introduced, assigning permissions according to predefined roles or user decisions. However, these models struggled to adapt in dynamic, large-scale environments, where multiple users required simultaneous access and updates. Insider threats and privilege escalation further weakened their effectiveness.

In parallel, digital signature and hashing techniques were adopted to maintain data integrity and verify authenticity. While effective in detecting alterations, they did not inherently prevent malicious updates before they occurred.

Recent developments focus on combining cryptographic techniques with layered verification models, where trustees or administrators review update requests before approval. Centralized monitoring tools have also been integrated to strengthen accountability and provide system-wide transparency. Although these methods have improved security, they still face challenges in scalability, real-time performance, and balancing security with user convenience.

PROPOSED SYSTEM

The proposed system introduces a secure framework designed to protect multi-user data updates through the integration of advanced encryption methods and layered access control. Unlike traditional systems that rely solely on passwords or single-step authentication, this framework incorporates encryption at every stage of data transmission and storage, ensuring confidentiality and integrity.

A trustee-based verification process is introduced, where update requests are validated before being finalized. This prevents unauthorized changes and provides accountability by requiring approval from trusted authorities. In addition, centralized administration allows continuous monitoring of user activity, ensuring that anomalies can be detected and mitigated promptly.

The system architecture defines clear roles for users, trustees, and administrators, minimizing risks of privilege misuse. By combining cryptography with controlled access and real-time monitoring, the framework delivers a reliable, scalable, and adaptable solution for safeguarding multi-user data updates in diverse organizational settings.

METHODOLOGY

The methodology for safeguarding multi-user data updates involves a structured, multi-layered process that integrates encryption, authentication, and trustee-based verification to ensure both security and usability. The system begins with user authentication, where credentials are securely validated before granting access. Each user is assigned specific roles and permissions, restricting actions to predefined boundaries and reducing risks of unauthorized activities.

Once authenticated, data update requests are processed through advanced encryption techniques. Symmetric encryption ensures efficient protection of stored data, while asymmetric encryption secures communication between users, trustees, and administrators. Hashing functions are employed to maintain data integrity, allowing detection of any unauthorized modifications.

Trustee-based verification acts as a second layer of defense. Before an update is finalized, the request is routed to a designated trustee or authority for approval. This step ensures accountability and prevents malicious or accidental data alterations.

Centralized administration plays a key role in monitoring activities across the system. Administrators can oversee user interactions, approve critical requests, and generate logs for auditing purposes. This provides transparency and enables quick identification of suspicious behavior.

This multi-stage process offers a balanced approach, addressing both technical and operational aspects of security, while providing scalability to adapt to organizational needs and future enhancements.

EXPERIMENTAL RESULTS

The experimental evaluation was carried out to validate the security, usability, and efficiency of the proposed system. The implementation demonstrated that key objectives, such as secure authentication, centralized administration, and controlled access to sensitive files, were effectively achieved.

The **User Login Page (Fig. 1)** acts as the primary access point. It restricts entry to registered users through secure credentials, while additional options like password recovery improve user convenience. The **Admin Home Page (Fig. 2)** provides centralized monitoring, where administrators can oversee activities, manage users, and approve requests. This layer of control ensures accountability and reduces the risk of misuse.

The **File Request and Verification Pages (Fig. 3 & Fig. 4)** illustrate the secure handling of data. Every request is validated through trustee and authority checks before granting access, ensuring that unauthorized modifications are prevented.

These results confirm that the system not only integrates security and accessibility but also offers reliability and scalability, making it a robust framework suitable for deployment in real-world scenarios.

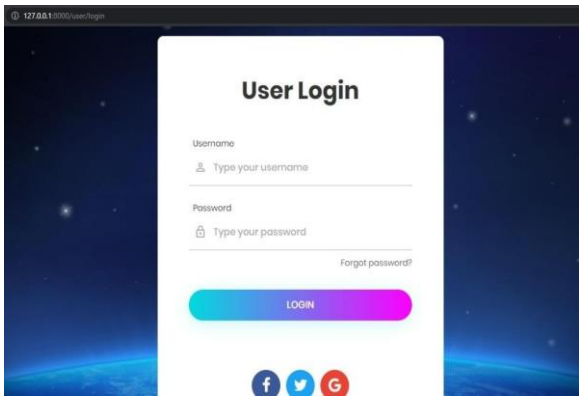

Fig 1: Login Page

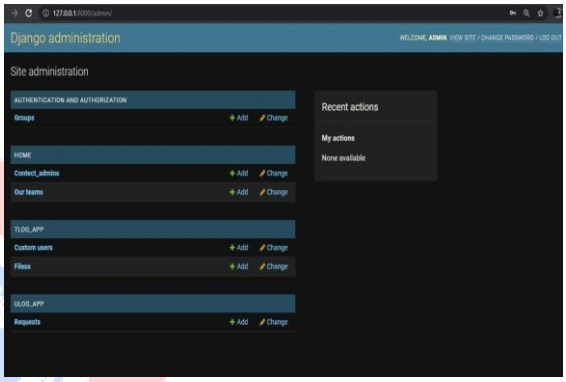

Fig 2: Admin Home Page

Fig 3: File Request

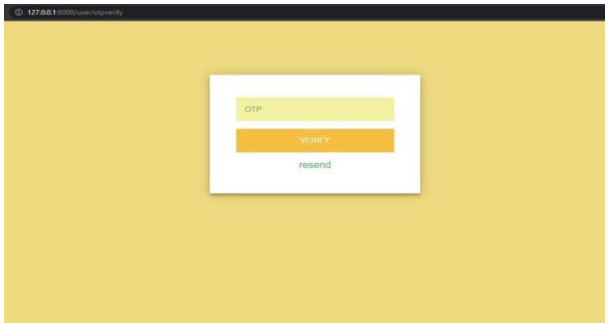

Fig 4: Verification page

CONCLUSION

This project demonstrates the successful design and implementation of a secure framework for safeguarding multi-user data updates using advanced encryption techniques. By integrating authentication, trustee-based verification, and centralized administration, the system ensures that sensitive information is accessible only to authorized individuals while maintaining efficiency. Clearly defined roles for users, trustees, and administrators establish accountability and minimize the possibility of unauthorized access or data misuse.

The modular structure of the framework enhances adaptability, making it suitable for organizations that require scalability and future upgrades without major redesign. Technologies such as Django, Bootstrap, and jQuery contributed to building a user-friendly interface that balances strong security with usability. Experimental evaluation further validated the reliability of the framework, showing consistent results in areas such as authentication, request validation, and administrative monitoring.

In addition to providing robust protection, the system also emphasizes practicality. Features such as password recovery, centralized oversight, and trustee-based approval ensure that the solution remains both secure and convenient for real-world use. Overall, the proposed system addresses the limitations of existing methods and offers an efficient, scalable approach for protecting multi-user environments. This makes it highly relevant for enterprises, educational institutions, and government platforms where secure data collaboration is essential.

REFERENCES

- A. Shamir, “Identity-Based Cryptosystems and Signature Schemes,” *Advances in Cryptology – CRYPTO*, Springer, 1984.
- D. Boneh and M. Franklin, “Identity-Based Encryption from the Weil Pairing,” *SIAM Journal on Computing*, vol. 32, no. 3, pp. 586–615, 2001.
- W. Stallings, *Cryptography and Network Security: Principles and Practice*, 8th Edition, Pearson, 2023.
- Django Software Foundation, *Django Documentation*. Available: https://www.djangoproject.com/
- Bootstrap, *Official Documentation*. Available: https://getbootstrap.com/