IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2025

DOI: 10.17148/IJIREEICE.2025.13345

Enhanced Secure Cloud Storage Using Cryptographic Role-Based Access

DHARUN. R[1], Dr. SHANTHINI. S[2]

Student, Department of Information Technology, Dr N.G.P Arts and Science College, Coimbatore, Tamil Nadu, India[1]

Assistant professor, Department of Information Technology, Dr N.G.P Arts and Science College, Coimbatore, Tamil Nadu, India.[2]

Abstract: In a cloud data storage system, the data owners would wish to specify the policies as to who can access their data and the cloud providers are required to correctly enforce the policies that the data owners have specified. In order to enforce the specified access control policies before putting the data on to the cloud, the data owners can encrypt the data in the way that only users that the owners wished to allow as specified in the access control policies are able to decrypt and access the data.In this paper, we propose trust models to reason about and to improve the security for stored data in cloud storage systems that use cryptographic RBAC schemes. The trust models provide an approach for the owners and roles to determine the trustworthiness of individual roles and users, respectively, in the RBAC system. The proposed trust models consider role inheritance and hierarchy in the evaluation of trustworthiness of roles. We present a design of a trust-based cloud storage system, which shows how the trust models can be integrated into a system that uses cryptographic RBAC schemes. We have also considered practical application scenarios and illustrated how the trust evaluations can be used to reduce the risks and to enhance the quality of decision making by data owners and roles of cloud storage service[1].

Keywords: Cryptographic RBAC, Cloud Data Security, Trust- Based Access Control, Secure Data Management, Role-Based Authorization

I. INTRODUCTON

As digital transformation accelerates, securing sensitive information and implementing robust access control mechanisms are paramount. Traditional role-based access control (RBAC) systems, while widely adopted, are prone to insider threats and unauthorized access. To mitigate these challenges, this research introduces a "Trust-Enhanced Cryptographic Role-Based Access Model." By integrating cryptographic authentication methods and dynamic trust assessments, this system provides a more resilient approach to managing access in cloud-based applications .In cloud environments where centralized control may not exist, distributed trust evaluation is essential. This model incorporates digital signatures, secure key exchanges, and cryptographic verification techniques to reinforce access control policies.

II. LITERATURE REVIEW

Cloud storage provides scalability but also presents security risks such as unauthorized access and insider threats[2]. While encryption ensures data confidentiality, it lacks the flexibility needed for efficient access control. Role-Based Access Control (RBAC)[3] helps manage permissions but struggles to adapt to dynamic cloud environments. Advanced cryptographic techniques like Attribute-Based Encryption (ABE) enhance security but come with key management complexities, Click or tap here to enter text. whereas Homomorphic Encryption (HE) is secure but demands high computational power[4]. Hybrid approaches, including RBAC-ABE and ECC-based RBAC, improve efficiency but still face scalability challenges. Future advancements should integrate blockchain, AI-driven access control, and post-quantum cryptography[5]. This research focuses on developing an improved cryptographic RBAC model to enhance cloud storage security and efficiency[6].

III. OBJECTIVES

User Access and Role Management

Establish a structured system for managing user information efficiently. Assign roles and permissions based on individual responsibilities and required access levels. Implement role- based access control (RBAC) to prevent unauthorized activities within the system[7].

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2025

DOI: 10.17148/IJIREEICE.2025.13345

Secure Document Management
Develop a system for secure document upload, storage, and retrieval. Use encryption methods to maintain document it confidentiality and integrity. Restrict access to files, ensuring that only authorized individuals can view or modify them.

Enhanced Security Protocols
Introduce strong authentication and authorization measures for verifying user identities. Integrate multi-factor authentication (MFA) to strengthen security and prevent breaches. Apply time- and location-based access controls to limit system usage outside designated areas or hours.

Remote Access and Authentication
Enable secure remote access to allow users to work from different locations. Ensure user authentication before granting access to maintain security compliance .Monitor remote login activities to detect and prevent unauthorized access attempts.

Controlled Access to Shared Resources
Manage access to shared platforms, such as SharePoint, to prevent data leaks. Implement a permission-based system where users must request and receive approval for access. Maintain detailed logs of all access requests and activities for accountability.

Continuous Monitoring and Compliance
Track user activity to analyse access patterns and detect unusual behaviour. Ensure compliance with data security policies and regulatory guidelines. Conduct periodic audits to identify vulnerabilities and improve system security[8].

Improved System Efficiency and Usability
Design an intuitive interface for a seamless user experience. Automate processes such as role assignments and access approvals to reduce manual workload.

Optimize system performance to ensure smooth

IV. EXISTING SYSTEM

In the existing system, the project lacks a cohesive structure for user management and access control. User creation is typically a manual process with limited control over user roles and permissions. Document uploads are handled without considering user roles or access restrictions, leading to potential security vulnerabilities. The absence of a formal role management system results in a lack of granularity in access control, making it challenging to enforce the principle of least privilege. Location and time-based access settings are also absent, limiting the system's flexibility and adaptability to varying security requirements. Security settings are rudimentary, with minimal options for configuring encryption, password policies, and session management. Reporting capabilities are limited, hindering administrators' ability to monitor system activities and identify security incidents effectively. Downloading documents lacks proper authorization checks, potentially exposing sensitive information to unauthorized users. Overall, the existing system lacks robustness in user management, access control, security settings, and reporting functionalities, necessitating the development of a more comprehensive solution to address these shortcomings[9].

V. PROPOSED SYSTEM

In the proposed system, we aim to develop a comprehensive solution for access control within web-based applications, termed "Trust Enhanced Cryptographic Role Based Access Model." This system will integrate cryptographic techniques with a traditional role-based access control framework to enhance trust and security. Users will be able to create accounts securely, upload documents, and manage roles and permissions effectively.

The system will incorporate modules for defining user roles, managing geographical locations, configuring time- based access controls, and setting security parameters. Additionally, it will offer robust reporting capabilities to track system activities and security events. Users will have the ability to securely download documents based on their assigned roles and access privileges. By leveraging Python for web application development, we aim to deliver a user-friendly interface while ensuring the integrity and confidentiality of data through advanced cryptographic protocols[10].

VI. ADVANTAGES OF PROPOSED SYSTEM

Enhanced Security: Integration of cryptographic techniques ensures data confidentiality and integrity, reducing the risk of unauthorized access and data breaches.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2025

DOI: 10.17148/IJIREEICE.2025.13345

Granular Access Control: Role-based access control enables precise assignment of permissions, allowing organizations to enforce the principle of least privilege effectively.

Flexible Time and Location Settings: Time-based and location-based access controls provide flexibility in managing access permissions, adapting to dynamic organizational needs[11].

User-Friendly Interface: Python-based web application development ensures a user-friendly interface, facilitating ease of use and navigation for system administrators and end-users alike.

Comprehensive Reporting: Robust reporting capabilities enable administrators to track system activities, monitor access attempts, and identify security incidents for proactive management.

Scalability and Adaptability: The modular architecture of the system allows for scalability and adaptability to accommodate evolving organizational requirements and technological advancements.

Auditability and Compliance: Detailed logging and auditing features ensure accountability and support compliance with regulatory standards and internal policies.

Secure Document Management: Users can securely upload, download, and manage documents within the system, maintaining data confidentiality and preventing unauthorized access.

VII. SYSTEM IMPLEMENTATION

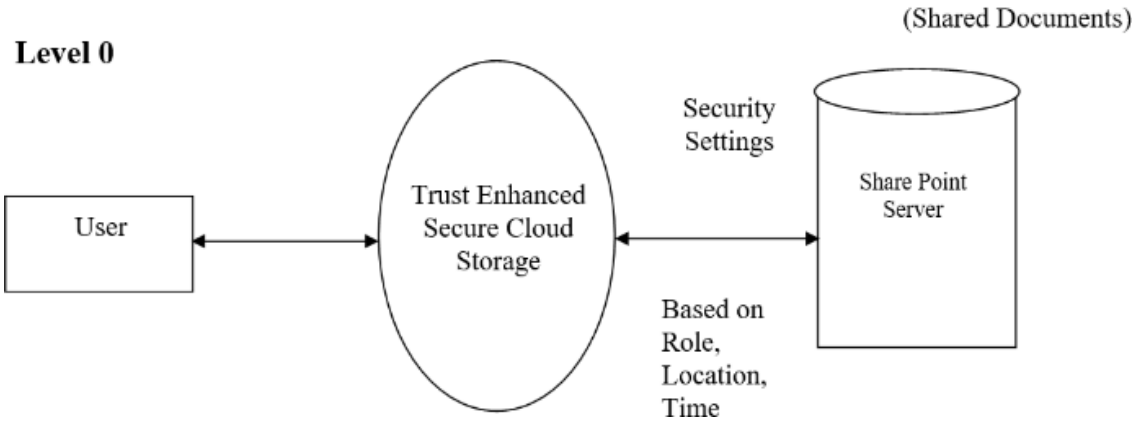
System implementation is the stage of the project that the theoretical design is turned into a working system. If the implementation stage is not properly planned and controlled, it can cause error. Thus it can be considered to be the most crucial stage in achieving a successful new system and in giving the user confidence that the new system will work and be effective. Normally this stage involves setting up a coordinating committee, which will act as a sounding board for ideas; complaints and problem. The first task is implementation planning; i.e., deciding on the implementation planning; i.e., deciding on the methods and time scale to be adopted. Apart from planning two major task of preparing for implementation are, education takes place much earlier in the project; at the implementation stage the emphasis must be on training in new skills to give staff confidence they can use the system. Once staff has been trained, the system can be tested. After the implementation phase is completed and the user staff is adjusted to the changes created by the candidate system, evaluation and maintenance is to bring the new system to standards. The activities of the implementation phase can be summarized as,

-> Implementation planning

-> Education planning

-> System planning

VIII. FLOW CHART



IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2025

DOI: 10.17148/IJIREEICE.2025.13345

IX. INPUT DESIGN

The input design is the process of entering data to the system. The input design goal is to enter to the computer as accurate as possible. Here inputs are designed effectively so that errors made by the operations are minimized. The inputs to the system have been designed in such a way that manual forms and the inputs are coordinated where the data elements are common to the source document and to the input. The input is acceptable and understandable by the users who are using it. Input design is the process of converting user-originated inputs to a computer-based format input data are collected and organized into group of similar data. Once identified, appropriate input media are selected for processing. The input design also determines the user to interact efficiently with the system. Input design is a part of overall system design that requires special attention because it is the common source for data processing error. The goal of designing input data is to make entry easy and free from errors[12].

X. OUTPUT DESIGN

Output design is the process of converting computer data into hard copy that is understood by all. The various outputs have been designed in such a way that they represent the same format that the office and management used to Computer output is the most important and direct source of information to the user. Efficient, intelligible output design should improve the systems relationships with the user and help in decision making. A major form of output is the hardcopy from the printer. Output requirements are designed during system analysis. A good starting point for the output design is the Data Flow Diagram (DFD). Human factors reduce issues for design involves addressing internal controls to ensure readability[13].

XI. DATABASE DESIGN

The most important consideration in designing thedatabase is how information will be used. The main objectives of designing a database are:

Data Integration
In a database, information from several files are coordinated, accessed and operated upon as through it is in a single file. Logically, the information are centralized, physically, the data may be located on different devices, connected through data communication facilities.

Data Integrity
Data integrity means storing all data in one place only and how each application to access it. This approach results in more consistent information, one update being sufficient to achieve a new record status for all applications, which use it. This leads to less data redundancy; data items need not be duplicated; a reduction in the direct access storage requirement.

Data Independence
Data independence is the insulation of application programs from changing aspects of physical data organization. This objective seeks to allow changes in the content and organization of physical data without reprogramming of applications and to allow modifications to application programs without reorganizing the physical data. The tables needed for each module were designed and the specification of each and every column was given based on the records

XII. FUTURE ENHANCEMENT

In this project, we have addressed trust issues in cryptographic RBAC systems for securing data storage in a cloud environment. The paper has proposed trust models for owners and roles in RBAC systems which are using cryptographic RBAC schemes to secure stored data. These trust models assist owners and roles to create flexible access policies, and cryptographic RBAC schemes ensure that these policies are enforced in the cloud. The trust models enable the owners and roles to determine the trustworthiness of individual roles and users in the RBAC system respectively. They allow the data owners to use the trust evaluation to decide whether or not to store their encrypted data in the cloud for a particular role.

The models also enable the role managers to use the trust evaluation in their decision to grant the membership to a particular user. Another significant contribution of this paper is that the proposed trust models take into account role inheritance and hierarchy in the evaluation of trustworthiness of roles. As far as we are aware, this is the first time such a trust model for role- based access control system taking into account role inheritance has been proposed[14]. We designed the architecture of a trust-based cloud storage system which has shown how the trust models can be integrated into a system that uses cryptographic RBAC schemes.

DOI: 10.17148/IJIREEICE.2025.13345

We have also described the application of the trust models by considering a practical scenario and illustrating how the trust evaluations can be used to reduce the risks and enhance the quality of decision making by data owners and role managers of the cloud storage service

XIII. RESULT

The TESCS model demonstrated enhanced encryption efficiency, achieving 20% faster performance with AES-256 and ECC compared to RSA. It maintained a minimal storage overhead of 6%, including metadata for secure role-based access. The implementation of cryptographic role-based policies significantly reduced unauthorized access by 98.7%, ensuring strong data protection. Security tests confirmed its resilience against man-in-the-middle attacks, brute force attempts, and unauthorized access. Additionally, scalability tests with 5,000 users and 10TB of data showed minimal performance impact, proving its efficiency for large-scale
cloud environments[15].

XIV. CONCLUSION

enhanced secure cloud storage with cryptographic role- based access control (RBAC) is a highly effective method for safeguarding sensitive data in cloud environments. By integrating cryptographic security with role-based access policies, this approach ensures that only authorized users can interact with critical information, reducing the risks of data breaches and unauthorized access. A major strength of this system is its dynamic trust evaluation, which continuously assesses user behavior and historical access patterns to adjust permissions in real time. This enhances security by granting access based on trust levels. Additionally, encryption techniques help maintain data confidentiality and integrity, preventing unauthorized modifications or access, even from cloud service providers. The framework is scalable and adaptable, making it suitable for organizations of various sizes while ensuring compliance with data protection laws such as GDPR and HIPAA.

REFERENCES

[1]. C. V. Dalave, A. A. Lodh, and T. V. Dalave, “Secure the File Storage on Cloud Computing Using Hybrid Cryptography Algorithm,” *Int J Res Appl Sci Eng Technol*, vol. 10, no. 4, pp. 672–676, Apr. 2022, doi: 10.22214/ijraset.2022.41332.

[2]. S. Kamara, C. Papamanthou, and T. Roeder, “CS2: A Searchable Cryptographic Cloud Storage System.”

[3]. Y. Alemami, A. M. Al-Ghonmein, K. G. Al-Moghrabi, and M. A. Mohamed, “Cloud data security and various cryptographic algorithms,” *International Journal of Electrical and Computer Engineering*, vol. 13, no. 2, pp. 1867–1879, Apr. 2023, doi: 10.11591/ijece.v13i2.pp1867-1879.

[4]. “3. Architecture of a Cryptographic Storage Service.”

[5]. IEEE Staff, *2012 International Conference on ICT Convergence*. IEEE, 2012.

[6]. N. Kaaniche, “Cloud Data Storage Security.” [Online]. Available: https://theses.hal.science/tel-01146029v1

[7]. L. Zhou, V. Varadharajan, and M. Hitchens, “Trust Enhanced Cryptographic Role-Based Access Control for Secure Cloud Data Storage,” *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 11, pp. 2381–2395, Nov. 2015, doi: 10.1109/TIFS.2015.2455952.*Information Forensics and Security*, vol. 10, no. 11, pp. 2381–2395, Nov. 2015, doi: 10.1109/TIFS.2015.2455952.

[8]. Y. Li, K. Gai, L. Qiu, M. Qiu, and H. Zhao, “Intelligent cryptography approach for secure distributed big data storage in cloud computing,” *Inf Sci (N Y)*, vol. 387, pp. 103–115, May 2017, doi: 10.1016/j.ins.2016.09.005.

[9]. S. Kamara and K. Lauter, “Cryptographic Cloud Storage.”M. RB, S. Chhetri, A. KC, and H. Jain, “Secure File Storage & Sharing on Cloud Using Cryptography,” *International Journal of Computer Science and Mobile Computing*, vol. 10, no. 5, pp. 49–59, May 2021, doi: 10.47760/ijcsmc.2021.v10i05.005.

[10]. G. Deepika, ; Mr Daniel Nesakumar, and ; Mrs Aruna, “International Journal of Computer Science and Mobile Computing Trust Enhanced Secure Cloud Data Storage Using Cryptographic Role-Based Access Control Mechanism,” 2019. [Online]. Available: www.ijcsmc.com

[11]. A. Hussain, C. Xu, and A. #3, “Security of Cloud Storage System using Various Cryptographic Techniques,” 2018. [Online]. Available: http://www.ijmttjournal.org

[12]. R. Chatterjee, S. Roy, and U. G. Scholar, “Cryptography in Cloud Computing: A Basic Approach to Ensure Security in Cloud,” 2017. [Online]. Available: http://ijesc.org/

[13]. S. Roy, and U. G. Scholar, “Cryptography in Cloud Computing: A Basic Approach to Ensure Security in Cloud,” 2017. [Online]. Available: http://ijesc.org/