Data Security Model for Cloud Computing Using VGRT Methodology

RAVINDAR MOGILI
Associate Professor
Dept. of Computer Science and Engineering
Jyothishmathi Institute of Technology and Science (JNTUH)
Karimnagar, Telangana, India
mogili.ravindar@jits.ac.in

SHASHIKANTH KANDUKURI
Associate Professor
Dept. of Computer Science and Engineering
Jyothishmathi Institute of Technology and Science (JNTUH)
Karimnagar, Telangana, India
shashi1215@gmail.com

POORNODAYA VADLAKONDA
Dept. of Computer Science and Engineering
UG Student
Jyothishmathi Institute of Technology and Science (JNTUH)
Karimnagar, Telangana, India
poornodaya2005@gmail.com

MOHAMMAD ABDUL RAQUEEB
Dept. of Computer Science and Engineering
UG Student
Jyothishmathi Institute of Technology and Science (JNTUH)
Karimnagar, Telangana, India
raqueebabdul8@gmail.com

PRASAD YEDAPALLI
Dept. of Computer Science and Engineering
UG Student
Jyothishmathi Institute of Technology and Science (JNTUH)
Karimnagar, Telangana, India
prasadyedapalli@gmail.com

RAJKUMAR KAMPELLY
Dept. of Computer Science and Engineering
UG Student
Jyothishmathi Institute of Technology and Science (JNTUH)
Karimnagar, Telangana, India
kampellyrajkumar3@gmail.com

VYSHNAVI CHINTHAKINDI
Dept. of Computer Science and Engineering
UG Student
Jyothishmathi Institute of Technology and Science (JNTUH)
Karimnagar, Telangana, India
chintakindivyshnavi@gmail.com

Abstract— **Cloud computing has become a popular solution for storing and managing data due to its flexibility, scalability, and cost-effectiveness. However, it also introduces significant challenges related to data security, access control, and trust, especially in multi-user environments. This paper presents a structured data security model based on the Verification–Generation–Retrieval–Trust (VGRT) methodology. The proposed approach ensures secure data handling by integrating four key components: verifying user identity, securely generating encrypted data, enabling controlled data retrieval, and establishing trust through data integrity validation. In this model, data is encrypted before storage, and access is granted only to authorized users through multi-user private key verification. A database is used to manage encrypted data and access-related information, ensuring transparency and control. Experimental results demonstrate that the proposed VGRT-based model significantly improves data confidentiality, access control, and trust in cloud computing environments.**

Keywords*— *cloud computing data security VGRT verification generation retrieval trust multi user key encryption access control

I. INTRODUCTION

Cloud computing has become an essential technology for delivering scalable computing resources and storage services over the internet. Organizations and individuals increasingly rely on cloud platforms to store sensitive data because of their flexibility, affordability, and ease of access. Despite these advantages, cloud computing introduces serious concerns regarding data security, user authentication, and trust. As multiple users access shared resources, ensuring that only authorized users can access sensitive data becomes a major challenge. Traditional security mechanisms such as basic encryption and authentication are no longer sufficient. Data must be protected throughout its lifecycle, including secure creation, proper verification, controlled access, and reliable retrieval. Weak verification or poor key management can lead to unauthorized access and reduced system reliability.

To address these issues, this paper proposes a data security model based on the VGRT methodology—Verification, Generation, Retrieval, and Trust. The model verifies users using secure private keys, encrypts data before storage, allows controlled retrieval for authorized users, and ensures trust by validating data integrity and usability. By combining these components into a unified framework, the VGRT model provides a structured and reliable approach to cloud data security. It enhances confidentiality, strengthens access control, and builds user trust, making it suitable for modern cloud environments.

II. LITERATURE SURVEY

Cloud security has been widely researched, with significant focus on data protection, user authentication, access control, and trust management. Existing studies emphasize the need to secure data across all stages of its lifecycle.

Several researchers highlight the importance of encryption techniques, including both symmetric and asymmetric methods, to protect sensitive data during storage and transmission. While these techniques ensure confidentiality, many systems rely only on encryption and fail to integrate it with other security processes.

User verification methods such as password-based systems, token-based authentication, and cryptographic key validation have also been explored. Multi-user verification using private keys has proven to be effective in controlling access. However, in many systems, verification is treated as a separate process rather than being integrated with data generation and retrieval.

Secure data retrieval mechanisms ensure that only authorized users can access encrypted data. Many approaches implement role-based or identity-based controls, but improper integration with other stages can lead to data inconsistency or misuse.

Trust is another critical factor in cloud computing. It is often established through data integrity checks, audit logs, and successful decryption. However, most existing models treat trust as an independent component instead of integrating it with the entire security workflow.

Overall, current research addresses individual aspects of cloud security but lacks a unified framework that integrates verification, generation, retrieval, and trust. This highlights the need for a structured VGRT-based model.

III. PROBLEM STATEMENT

With the rapid growth of cloud computing, large volumes of sensitive data are generated, stored, and accessed remotely. While cloud platforms provide convenience and scalability, ensuring secure data handling across multiple users remains a major challenge. Many existing cloud systems lack a structured mechanism to manage secure data generation, user verification, controlled data retrieval, and trust establishment in an integrated manner.

Current approaches often implement encryption, authentication, or access control as independent components. These fragmented solutions fail to guarantee that data generated in the cloud is consistently verified, securely retrieved, and trusted during actual usage. In multi-user environments, improper key validation and uncontrolled retrieval can lead to unauthorized access or data misuse. Additionally, users have limited assurance that retrieved data is authentic, intact, and usable.

Therefore, there is a need for a unified VGRT-based cloud data security model that ensures:

Secure generation of encrypted data and keys
Strong verification of authorized users
Controlled and accurate retrieval of stored data
Establishment of trust through successful data integrity and usability

The objective of this project is to design and implement a cloud data security system based on Verification, Generation, Retrieval, and Trust (VGRT) that provides end-to-end protection and reliable access to cloud-stored data in a multi-user environment.

IV. EXISTING AND PROPOSED SYSTEM

A. Existing System

In existing cloud systems, security mechanisms are often unstructured and fragmented. Data encryption, user authentication, data retrieval, and trust are handled independently.

Most systems focus mainly on encryption but lack strong verification mechanisms. Authentication is typically limited to usernames and passwords, which may not provide sufficient security.

During data retrieval, minimal validation increases the risk of unauthorized access. Trust is often assumed rather than verified, and users have limited assurance about data integrity.

B. Proposed System

The proposed system introduces a unified VGRT-based security model that integrates all four components into a single workflow.

- Generation: Files are encrypted before storage using secure cryptographic techniques.
- Verification: Users are authenticated using multi-user private key validation.
- Retrieval: Data is accessed only after successful verification and is securely decrypted.
- Trust: Data integrity and usability are validated to ensure reliability.

MongoDB is used to store encrypted data, user credentials, and access logs, improving transparency and control.

This integrated approach ensures better security, reliability, and trust compared to traditional systems.

V. SYSTEM ARCHITECTURE

Fig.5.1 System Architecture

The system architecture is designed to implement the VGRT workflow through multiple interconnected modules:

- User Interface Module: Allows users to upload, access, and retrieve files.
- Generation Module: Encrypts files and generates secure keys.
- Verification Module: Authenticates users using private keys.
- Storage Module: Stores encrypted files and metadata in MongoDB.
- Retrieval Module: Decrypts data for authorized users.
- Trust Module: Validates data integrity and usability.

All modules work together to ensure secure data flow and controlled access.

VI. PROPOSED METHOD IMPLEMENTATION AND ALGORITHMS

The proposed method implements a structured Verification–Generation–Retrieval–Trust (VGRT) workflow to ensure secure cloud-based data storage and controlled access. Each phase of the VGRT methodology is designed to address specific security challenges in cloud environments and is tightly integrated to provide end-to-end data protection.

A. Verification Phase

The verification phase authenticates users before allowing any operation on cloud-stored data. User identity is validated using private key credentials, ensuring that only authorized users can proceed. Multi-user verification prevents unauthorized access and strengthens access control in shared cloud environments.

B. Generation Phase

In the generation phase, user-uploaded files are securely processed before storage. The system encrypts files using cryptographic algorithms and converts them into encrypted binary (.bin) format. Encryption keys are generated and securely managed, ensuring data confidentiality at the time of creation and storage.

C. Retrieval Phase

The retrieval phase allows authorized users to access encrypted data only after successful verification. The system performs controlled decryption using valid cryptographic keys and restores the original file format. This phase ensures data accuracy and prevents corruption during retrieval.

D. Trust Phase

The trust phase validates the integrity and usability of retrieved data. Successfully decrypted files are verified by correct opening and usage, confirming that the data remains intact and authentic. Access logs and metadata maintained in the database further enhance transparency and trustworthiness.

Algorithm :

1 VGRT-Based Secure Data Handling
2 User uploads a file to the system.
3 System verifies user identity using private key authentication.
4 Encryption keys are generated or retrieved securely.
5 File is encrypted and converted into binary format.
6 Encrypted file and metadata are stored in the cloud database.
7 Upon access request, user verification is revalidated.
8 Encrypted file is retrieved and decrypted securely.
9 File integrity and usability are verified to establish trust.

VII. RESULT ANALYSIS

The proposed system was tested to evaluate its effectiveness in ensuring secure data handling.

- The verification module successfully prevented unauthorized access
- Files were securely encrypted and stored without exposing plaintext data
- MongoDB efficiently managed data and access logs
- Only authorized users could retrieve and decrypt files
- Retrieved files- maintained integrity and usability

The results confirm that the VGRT model improves confidentiality, access control, and trust in cloud systems.

Fig-7.1 Result Analysis

Secure User Login Interface for Multi-User Verification The figure illustrates the secure user login interface used in the proposed VGRT-based cloud data security model. The interface enables user authentication through username and password credentials before granting access to cloud resources. Upon successful verification, users are authenticated using private key–based validation, ensuring that only authorized users can

proceed to data generation, retrieval, and trust establishment phases. This login mechanism supports multi-user access control and strengthens the verification component of the VGRT methodology.

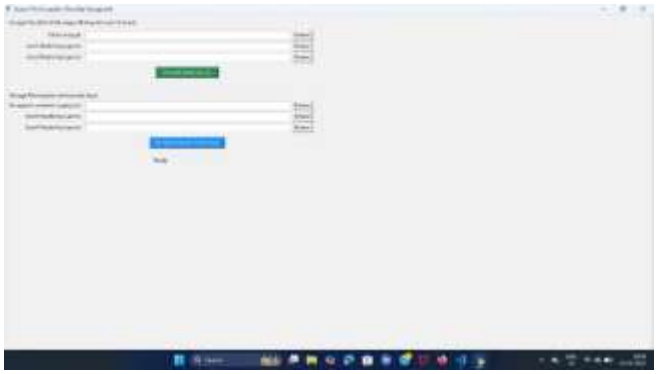

Fig-7.2 Result Analysis

The figure illustrates the secure file encryption and decryption interface implemented as part of the proposed VGRT-based cloud data security model. The interface supports multi-user key-based encryption, where a single file is encrypted using symmetric encryption and the encryption key is securely wrapped for multiple authorized users.

During the Generation phase, the user selects a file for encryption along with the public keys of authorized users. The system applies AES-GCM encryption to protect the file content and wraps the encryption key separately for each user using their respective public keys. This ensures that only intended users can later access the encrypted data.

In the Retrieval phase, the encrypted container file is selected along with the corresponding private keys of the authorized users. Decryption is permitted only when all required private keys are successfully validated. The system then unwraps the encryption key and restores the original file without data loss or corruption.

This mechanism enforces multi-user access control, prevents unauthorized decryption, and strengthens the Verification and Trust components of the VGRT methodology. The successful completion of encryption and decryption operations confirms data confidentiality, integrity, and controlled access in the cloud environment.

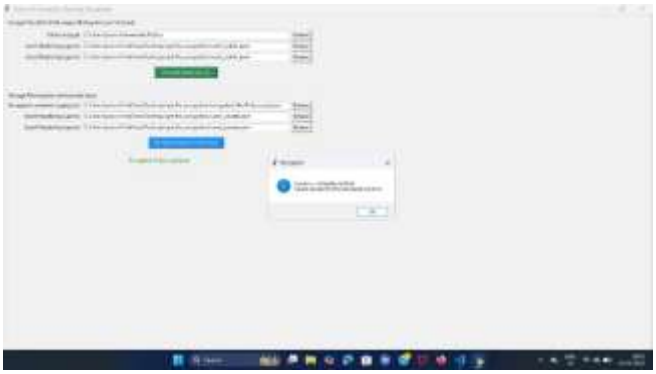

Fig-7.3 Result Analysis

The figure demonstrates the successful execution of the multi-user encryption and decryption process implemented under the proposed VGRT-based cloud data security model. During the Generation phase, a user-selected document file is encrypted using the AES-GCM algorithm, ensuring confidentiality and integrity of the data. The symmetric encryption key is securely wrapped using the public keys of two authorized users, enabling multi-user access control.

The encrypted output is stored as a secure container file in VGRT JSON format, which encapsulates the encrypted data, wrapped keys, and integrity verification information. This container format ensures that the encrypted data remains protected during storage and transmission in the cloud environment.

In the Retrieval phase, the encrypted container is accessed only after successful verification of both users through their corresponding private keys. The system validates the private keys, unwraps the encryption key, and performs controlled decryption. As shown in the figure, decryption is completed successfully only when both private keys are provided.

The confirmation message indicating successful decryption and integrity verification confirms that the retrieved file matches the original data without corruption or modification. This outcome validates the Trust phase of the VGRT methodology, ensuring data authenticity, integrity, and reliable access.

Overall, the experimental results confirm that the proposed system effectively enforces multi-user authorization, prevents unauthorized access, and guarantees secure data generation, retrieval, and trust establishment in cloud computing environments.

VIII. CONCLUSION

This paper presented a VGRT-based cloud data security model that integrates verification, generation, retrieval, and trust into a unified framework.
The model ensures secure data handling by combining strong user authentication, encryption, controlled access, and integrity validation. Experimental results show that it effectively prevents unauthorized access and maintains data reliability.
Overall, the proposed system provides a scalable and secure solution for cloud data management and can be applied to various real-world applications.

REFERENCES

[1] P. Mell and T. Grance, “The NIST definition of cloud computing,” National Institute of Standards and Technology (NIST), Special Publication 800-145, 2011.
[2] M. Armbrust *et al.*, “A view of cloud computing,” *Communications of the ACM*, vol. 53, no. 4, pp. 50–58, 2010.
[3] K. Hashizume, D. G. Rosado, E. Fernandez-Medina, and E. B. Fernan-´ dez, “An analysis of security issues for cloud computing,” *Journal of Internet Services and Applications*, vol. 4, no. 1, pp. 1–13, 2013.
[4] S. Subashini and V. Kavitha, “A survey on security issues in service delivery models of cloud computing,”

Journal of Network and Computer Applications, vol. 34, no. 1, pp. 1–11, 2011

[5] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed. Pearson Education, 2017.

[6] D. Boneh and V. Shoup, *A Graduate Course in Applied Cryptography*. Stanford University, 2020.

[7] R. Buyya, C. S. Yeo, and S. Venugopal, "Market-oriented cloud computing: Vision, hype, and reality," in *Proc. IEEE Int. Conf. High Performance Computing and Communications*, 2008, pp. 5–13.

[8] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proc. Annual Int. Conf. on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*, 2005, pp. 457–473.

[9] IEEE Computer Society, "IEEE standard for cloud computing security," IEEE Standards, 2019.