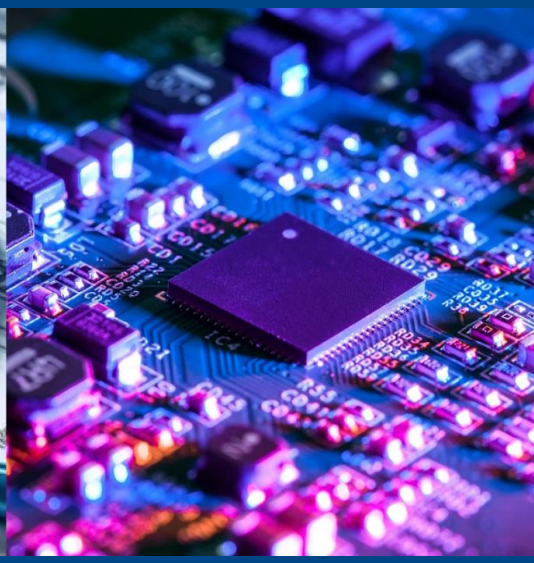
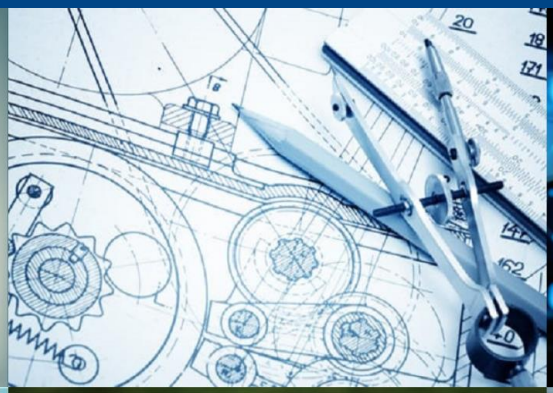
ISSN: 2582-7219

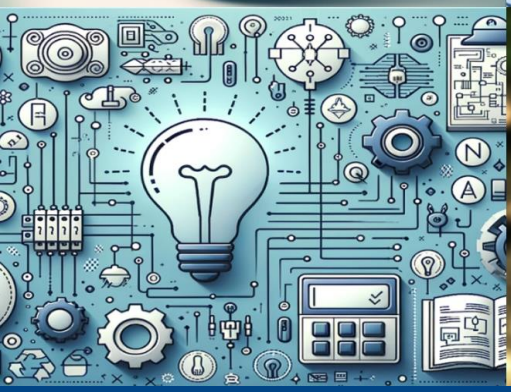




International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206 **Volume 8, Issue 3, March 2025**

© 2025 IJMRSET | Volume 8, Issue 3, March 2025| DOI: 10.15680/IJMRSET.2025.0803232

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Secure and Efficient Fine Grained Access Control for Cloud Storage using Blockchain

Dr. D.J. Samatha Naidu, K. Venkata Ramya, Venkata Sai Ganesh

Professor, Dept. of MCA, APGCCS, Ramajpet, Andhra Pradesh, India

Assistant Professor, Dept. of MCA, APGCCS, Ramajpet, Andhra Pradesh, India

PG Student, Dept. of MCA, APGCCS, Ramajpet, Andhra Pradesh, India

ABSTRACT: Digital Investigation on the cloud platform is a challenging task. Preservation of evidences is the ultimate goal behind performing cloud forensics. In the Virtual Scenario, Virtual Machines contain evidences. If once VMDK (Virtual Machine Disk file) is destroyed, it is impossible to recover your VM. At present there does not exist a single mechanism that can recover a destroyed (deleted) VM again which is the flaw in VM itself. All the activities on the VM is logged in VM, whereas activities of CSP (Cloud Service Provider) is logged on the server. So even if someone deleted the VM, all the evidences will be lost. This creates a disaster for the user and acts as a barrier for a forensic investigator to dig out the private crucial data of user that was stored in the Virtual Machine sometime. We proposed with this research work, we explore the existing mechanisms and challenges in the current cloud scenario and propose an idea to prevent the unauthorized deletion of the Virtual Machines snapshots.

I. INTRODUCTION

The rapid development of cloud storage services has attracted widespread attention from academia and industry owing to certain advantages such as always being turned on, a low cost, and flexible access. Users can outsource data, including personal and business documents, to cloud storage and share them. However, the data security issues that arise are not to be overlooked. Finding a way to ensure data security while maintaining the convenience of data sharing has become an urgent problem for cloud storage services. Attribute-based encryption (ABE) offers an effective solution to this challenge.

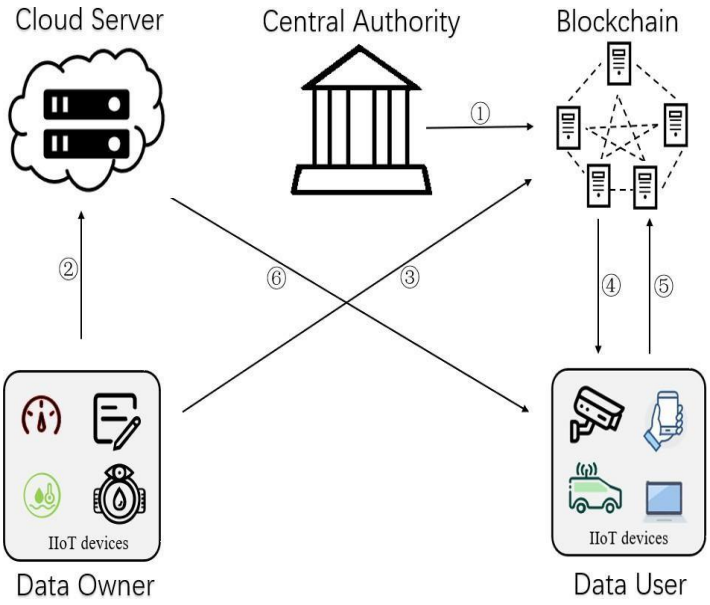


Figure 1: System Architecture

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

II. LITERATURE REVIEW

A **literature survey** on "Secured and Efficient Fine-Grained Access Control for Cloud Storage Using Blockchain" would explore the intersection of cloud storage security, access control, and blockchain technology, focusing on methods that ensure fine-grained control over access while maintaining high levels of security and efficiency. Below is a breakdown of key concepts, technologies, and research trends in this area:

1. Cloud Storage Security and Access Control

Cloud storage offers a flexible and scalable way to store data, but it also introduces several security challenges, especially regarding data access control. Traditional methods of access control (like role-based access control, or RBAC) may not be fine-grained enough for highly sensitive data or data that requires varying levels of access by different users.

Key Issues in Cloud Storage Security:

Data Privacy: Sensitive data must be protected from unauthorized access.

Data Integrity: Data must not be tampered with during storage or transmission.

Access Control Granularity: Users need different levels of access (e.g., read, write, modify, delete), and the cloud storage system must handle these granular permissions efficiently.

Existing Access Control Models:

- **Role-Based Access Control (RBAC):** While useful, RBAC lacks the fine-grained control needed for dynamic environments.
- **Attribute-Based Access Control (ABAC):** ABAC uses attributes (e.g., user's role, time, location) for access control but can become cumbersome and difficult to manage at scale.
- **Cryptographic Techniques:** Homomorphic encryption and proxy re-encryption are often employed to protect data confidentiality while allowing fine-grained access control.

2. Blockchain Technology in Cloud Storage

Blockchain provides a decentralized, transparent, and immutable ledger that can address many issues in cloud storage, particularly regarding access control and auditing.

Blockchain Benefits in Cloud Storage:

- **Decentralization:** Reduces the dependency on a central authority, which can be a point of failure or attack.
- **Transparency and Accountability:** Blockchain's immutable ledger allows tracking all access requests and changes, providing an audit trail.
- **Smart Contracts:** These can automate and enforce access control policies based on predefined conditions, ensuring secure access to cloud-stored data.

Blockchain-Based Access Control Models:

- **Smart Contract-Based Control:** Smart contracts on the blockchain can enforce access policies, ensuring only authorized users access the data. The policies can be fine-grained (e.g., based on user attributes, time, location, etc.).
- **Permissioned Blockchain:** A permissioned blockchain can be used where only authorized participants are allowed to read or write to the blockchain. This can be particularly useful in cloud storage to ensure access control without compromising privacy.

3. Fine-Grained Access Control Using Blockchain

Fine-grained access control ensures that different users can have different levels of access to different parts of a stored object (e.g., read/write permissions for specific file segments or blocks).

Blockchain-Enabled Fine-Grained Access Control Approaches:

- **Attribute-Based Encryption (ABE) with Blockchain:** Attribute-based encryption schemes can provide fine-grained access control by allowing data encryption based on user attributes. The blockchain can store and validate access requests, enabling automated access control.
- **Tokenization and Blockchain:** Users can be granted access to certain resources via tokens stored on the blockchain. These tokens can represent different levels of access or permissions and can be transferred or revoked as needed.
- **Access Control Lists (ACLs) and Blockchain:** Blockchain can store and manage dynamic ACLs, where each user has specific access rights to certain data. The ledger's immutability ensures that these access rights are tamper-proof.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

4. Blockchain-Based Solutions for Efficiency and Scalability

Although blockchain introduces several benefits, its inherent characteristics (e.g., computational overhead, consensus mechanisms) can impact efficiency. For cloud storage, it's crucial to balance security and efficiency.

Efficiency Challenges:

- **High Latency and Transaction Costs:** The consensus mechanism in traditional blockchains (e.g., proof-of-work) can incur high transaction costs and delays, which can hinder performance.
- **Scalability:** Cloud storage systems must be scalable to handle large amounts of data. Blockchain systems, particularly public blockchains, can struggle to scale due to the overhead involved in transaction validation.
- **Data Storage on Blockchain:** Storing large amounts of data directly on a blockchain is impractical due to storage and cost limitations. Instead, **off-chain storage** is typically used, where metadata (access permissions, logs, etc.) is stored on-chain, and actual data is stored off-chain.

Solutions for Improved Efficiency:

- **Sidechains and Layer-2 Solutions:** These solutions allow transactions and data management to occur off the main blockchain, reducing congestion and improving scalability.
- **Inter-Blockchain Communication:** Integrating multiple blockchains (e.g., permissioned chains for access control and public chains for data storage) can provide a more efficient architecture for cloud storage.
- **Hybrid Systems:** Combining traditional cloud storage systems with blockchain for specific tasks like access control and auditing while maintaining performance.

5. Recent Research and Developments

Several studies have emerged in recent years proposing novel blockchain-based methods for secure and fine-grained access control in cloud storage. Key advancements include:

- **Decentralized Access Control using Blockchain and Smart Contracts:** Smart contracts are used to automatically enforce access policies, reducing human intervention and improving the security of access management.
- **Blockchain-Based Data Provenance:** Blockchain can track the history of data access and modifications, allowing for transparent auditing and traceability, which is especially useful in regulated environments (e.g., healthcare, finance).
- **Zero-Knowledge Proofs:** Combining zero-knowledge proofs with blockchain can provide privacy-preserving fine-grained access control, where the verifier does not learn anything about the data except for the fact that the user is authorized.

6. Challenges and Future Directions

- **Interoperability:** Blockchain platforms are still fragmented, and integrating various blockchain systems with cloud storage systems remains challenging.
- **User Experience:** Blockchain systems may require users to manage cryptographic keys and tokens, which can introduce complexity. Efforts are being made to improve the usability of blockchain-based systems for end-users.
- **Regulatory Compliance:** Blockchain's decentralized nature could clash with existing regulations regarding data storage, access control, and privacy. Compliance with GDPR, HIPAA, and other data protection laws will need to be addressed.

III. METHODOLOGY OF PROPOSED SURVEY

The Software Development Life Cycle (SDLC) is a series of stages that provide a structured approach to the software development process. It encompasses understanding the business requirements, eliciting needs, converting concepts into functionalities and features, and ultimately delivering a product that meets business needs. A proficient software developer should possess adequate knowledge to select the appropriate SDLC model based on project context and business requirements.

Therefore, it is essential to select the right SDLC model tailored to the specific concerns and requirements of the project to ensure its success. To explore more about choosing the right SDLC model, you can follow this link for additional information. Furthermore, software lifecycle testing and SDLC stages, follow the highlighted links here.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

The exploration will cover various types of SDLC models, their benefits, disadvantages, and when to use them. SDLC models can be viewed as tools to enhance product delivery. Therefore, understanding each model, Its advantages, disadvantages, and the appropriate usage is crucial to determine which one suits the project.
The SDLC methodology usually contains the following stages:

1. Requirement Gathering
2. System Design
3. Implementation
4. Testing
5. Deployment
6. Maintenance

SDLC stands for Software Development Life Cycle. A Software Development Life Cycle is essentially a series of steps, or phases, that provide a model for the development and lifecycle management of an application or piece of software. The methodology within the SDLC process can vary across industries and organizations, but standards such as ISO/IEC 12207 represent processes that establish a lifecycle for software, and provide a mode for the development, acquisition, and configuration of software systems. SDLC consists of following activities: The sequential phases in Waterfall model are:

Requirement Gathering and analysis
All possible requirements of the system to be developed are captured in this phase and documented in a requirement specification.
System Design
The requirement specifications from first phase are studied in this phase and system design is prepared. System Design helps in specifying hardware and system requirements and also helps in defining overall system architecture.
Implementation
With inputs from system design, the system is first developed in small programs called units, which are integrated in the next phase.Each unit is developed and tested for its functionality which is referred to as Unit Testing.
Integration and Testing
All the units developed in the implementation phase are integrated into a system after testing of each unit. Post integration the entire system is tested for any faults and failures.
Deployment of system
Once the functional and non-functional testing is done, the product is deployed in the customer environment or released into the market.
Maintenance
There are some issues which come up in the client environment. To fix those issues patches are released. Also to enhance the product some better versions are released. Maintenance is done to deliver these changes in the customer environment.

Advantages

- The waterfall model is a simple model.
- It is easily understood as all the phases are done by step by step.
- No complexity as the deliverables of each phase are well defined.

Disadvantages

- This model cannot be used for the Project wherein the requirement is not.
- Clear or the requirement keeps on changing.
- A working model can only be available once the software reaches at last stage of the cycle.
- It is a time-consuming mode.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

IV. CONCLUSION AND FUTURE WORK

The proposed a novel scheme to transfer user data between different cloud servers based on a key agreement protocol. Through the mathematical analysis and comparative evaluation presented in this paper, the advantages of our scheme are proved from three aspects: security performance, calculation costs and communication costs. Our proposed scheme can efficiently solve the primary problem of trust during data migration between cloud servers and further can provide anonymity for the identity of cloud servers. On the premise of protecting the privacy of cloud service providers, our proposed scheme indirectly protects the privacy of users. In addition, the identity traceability provided by our proposed scheme also enables users to effectively constrain the cloud service providers.

The proposed scheme can be extended to support multi-cloud collaboration, enabling seamless data transfers across hybrid and edge-cloud environments while maintaining security and performance. An adaptive key management mechanism could further enhance security by dynamically refreshing encryption keys without disrupting data migration. Additionally, integrating AI-driven anomaly detection can provide real-time monitoring to identify and mitigate potential breaches during data transfers. To future-proof the system, incorporating quantum-resistant cryptography ensures resilience against emerging quantum computing threats.

REFERENCES

1. Java Crash Course 2nd Edition - this is a basic level book for beginners.
2. Learning java 5th Edition - this book is a practical learning book for basic to advanced level.
3. Java Cookbook - this book for advanced programmer interested in learning about modern java development tools.
4. Automating Boring Stuff With Java - In this book you will learn to write programs in java.
5. Head First Java - this book covered the fundamental of java.
6. Think Java - the basics of programming concepts and cover advanced topics like data structure and object-oriented design.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com