VISVESVARAYA TECHNOLOGICAL UNIVERSITY

"Jnana Sangama", Belgaum-590 014, Karnataka.

A
Technical Seminar Report
On

"Secure Data Storage and Sharing Techniques for Data Protection in Cloud Environment"

Submitted in the partial fulfillment of the requirements for the award of the Degree of

BACHELOR OF ENGINEERING
IN
INFORMATION SCIENCE AND ENGINEERING

Submitted by

PRAJWAL L H
1EW20IS055

Under the Guidance of

Mrs. Padmaja
Assistant Professor

EAST WEST INSTITUTE OF TECHNOLOGY

DEPARTMENT OF INFORMATION SCIENCE AND ENGINEERING

EAST WEST INSTITUTE OF TECHNOLOGY

BANGALORE - 560 091
2023-2024

EAST WEST INSTITUTE OF TECHNOLOGY

Sy. No.63,Off. Magadi Road, Vishwaneedam Post, Bangalore - 560 091
(Affiliated To Visvesvaraya Technological University, Belgaum)

DEPARTMENT OF INFORMATION SCIENCE AND ENGINEERING

EAST WEST
INSTITUTE OF
TECHNOLOGY

CERTIFICATE

This is to certify that the Technical Seminar work entitled **"Secure Data Storage and Sharing Techniques for Data Protection in Cloud Environment"** presented by **PRAJWAL L H, 1EW20IS055,** bonafide student of **EAST WEST INSTITUTE OF TECHNOLOGY**, Bangalore in partial fulfillment for the award of **Bachelor of Engineering** in **Information Science and Engineering** of **Visvesvaraya Technological University**, Belgaum during the year **2023-2024**. It is certified that all corrections/suggestions indicated have been incorporated in the report. The technical seminar has been approved as it satisfies the academic requirements in respect of technical seminar project prescribed for the said degree.

Signature of Internal Guide	Signature of HOD	Signature of Principal
Mrs. Padmaja	**Dr Suresh M B**	**Dr. K Channakeshavalu**
Assistant Prof, Dept. of ISE	Prof & Head, Dept. of ISE	Principal
EWIT, Bangalore	EWIT, Bangalore	EWIT, Bangalore

External Viva

Name of the Examiners	**Signature with date**
1. _____	_____
2. _____	_____

EAST WEST INSTITUTE OF TECHNOLOGY

Sy. No.63,Off. Magadi Road, Vishwaneedam Post, Bangalore - 560 091
(Affiliated To Visvesvaraya Technological University, Belgaum)

DEPARTMENT OF INFORMATION SCIENCE AND ENGINEERING

DECLARATION

I, **Prajwal L H**, student of Eight Semester, B.E in Information Science & Engineering, East West Institute of Technology, Bengaluru, hereby declare that the technical seminar entitled "The Role of Security in Human-Robot Shared Environments: A Case Study in ROS-based Surveillance Robots" has been independently carried out by me and submitted in the partial fulfillment of the requirement for the award of Bachelor of Engineering degree in Information Science & Engineering by Visvesvaraya Technological University, Belgaum during the academic year 2023-2024. Further the matter embodied in the dissertation has not been submitted previously by anybody for the award of any degree or diploma to any other University.

Place: Bengaluru **PRAJWAL L H**

Date: 04/03/2024 **1EW20IS055**

ABSTRACT

The rapid adoption of cloud computing has revolutionized the way organizations store, manage, and share data. However, with the benefits of cloud storage come significant security challenges, particularly concerning data protection. This report explores various techniques and strategies for secure data storage and sharing in cloud environments to mitigate the risks associated with unauthorized access, data breaches, and other security threats. The report begins by outlining the fundamental principles of cloud computing and the essential components of cloud-based data storage systems. It then delves into the specific security challenges faced by organizations in the cloud, including data privacy concerns, compliance requirements, and the shared responsibility model between cloud providers and users.

ACKNOWLEDGEMENT

Any achievement, be it scholastic or otherwise does not depend solely on the individual efforts but on the guidance, encouragement and cooperation of intellectuals, elders and friends. A number of personalities, in their own capacities have helped me in carrying out this project work. We would like to take this opportunity to thank them all.

First and foremost, I would like to thank **Dr. K Channakeshavalu**, Principal, EWIT, Bangalore, for his moral support towards completing our project work.

I would like to thank, **Dr. Suresh M B,** Professor and Head of Department of ISE, EWIT, Bangalore, for his valuable suggestions and expert advice.

I deeply express our sincere gratitude to our guide **Mrs. Padmaja K**, *Assistant Professor*, Department of ISE, EWIT, Bangalore for her able guidance throughout the project work and guiding me to organize the report in a systematic manner.

I thank my Parents, and all the faculty members of Department of Information science & Engineering for their constant support and encouragement.

Last, but not the least, I would like to thank my peers and friends who provided me with valuable suggestions to improve my technical seminar project.

PRAJWAL LH
1EW20IS055

TABLE OF CONTENTS

LIST OF FIGURES

Chapter 1

INTRODUCTION

Data defines the uniqueness of every enterprise. It is the main foundation of information, knowledge, and ultimately the wisdom for correct decisions and actions.Cloud computing is a paradigm that enables huge memory space and massive computation capacity at a low cost .It allows users to obtain the intended services across multiple platforms irrespective of location and time and consequently conveys an extensive convenience to the cloud users .By migrating the local data management system into cloud storage and using cloud-based services, users can accomplish cost savings and productivity enhancements to manage projects and establish collaborations. Most businesses have shifted to the cloud for these services due to its several advantages such as on-demand service, scalability, reliability, elasticity, measured services, disaster recovery, accessibility, and many others. Encryption plays a central role in secure data storage and sharing. By encrypting data both at rest and in transit, sensitive information is rendered unreadable to unauthorized users, thereby minimizing the risk of data exposure. Additionally, access control mechanisms such as role-based access control (RBAC) and multi-factor authentication (MFA) help enforce strict access policies, ensuring that only authorized individuals can access and manipulate data within the cloud. Furthermore, data anonymization and pseudonymization techniques can be employed to protect privacy and comply with regulatory requirements such as GDPR (General Data Protection Regulation) and HIPAA (Health Insurance Portability and Accountability Act). These techniques involve masking or obfuscating personally identifiable information (PII) to prevent unauthorized identification of individuals.

Chapter 2

EXISTING SYSTEM

The existing systems and technologies for secure data storage and sharing techniques in cloud environments are diverse and continually evolving to address the growing challenges of data protection. Here are some of the key existing systems and approaches:

1. **Encryption Technologies**:

- **Transport Layer Security (TLS)/Secure Sockets Layer (SSL):** Used for securing data in transit between clients and cloud servers, ensuring confidentiality and integrity.
- **Advanced Encryption Standard (AES):** A widely adopted symmetric encryption algorithm for encrypting data at rest, providing strong protection against unauthorized access.

2. **Access Control Mechanisms:**

- **Role-Based Access Control (RBAC):** Assigns permissions and access rights based on users' roles within an organization, limiting access to data based on predefined roles.
- **Attribute-Based Access Control (ABAC**): Determines access based on user attributes, environmental conditions, and policies, offering more granular access controls.

3. **Data Masking and Tokenization:**

- **Data Masking:** Techniques like masking sensitive data elements (e.g., replacing real values with masked values) in non-production environments to protect data during development and testing.
- **Tokenization:** Replaces sensitive data with non-sensitive placeholders (tokens) that are meaningless without the tokenization system, enhancing data protection during storage and transmission.

4. **Secure File Sharing Platforms**:

- **Box, Dropbox, Google Drive:** These platforms offer encryption, access controls, audit trails, and secure sharing features to protect data shared among authorized users.
- **Microsoft OneDrive:** Integrates encryption, access controls, and collaboration tools for secure file storage and sharing in cloud environments.

5. **Digital Rights Management (DRM) Solutions:**

- Microsoft Azure Information Protection: Provides encryption, access controls, and rights management capabilities to protect sensitive data and control its usage, even when shared outside the organization.
- **Adobe Digital Rights Management:** Offers encryption, permissions, and policies for protecting digital content (e.g., documents, images, videos) and managing access rights.

6. **Cloud Access Security Brokers (CASBs):**

- **Netskope, Bitglass, Cloudflare:** CASBs provide visibility, control, and security enforcement for cloud applications, offering features like data encryption, access controls, threat detection, and compliance monitoring.

7. **Data Loss Prevention (DLP) Solutions:**

- **Symantec Data Loss Prevention, McAfee DLP**: These solutions monitor, detect, and prevent data breaches by identifying sensitive data, enforcing policies, and blocking unauthorized data transfers or leaks.

8. **Blockchain Technology:**

- **Hyperledger Fabric, Ethereum:** Blockchain-based solutions offer decentralized and immutable data storage, ensuring data integrity, transparency, and auditability for sensitive transactions and records.

9. **Homomorphic Encryption:**

- IBM Fully Homomorphic Encryption Toolkit: Enables computations on encrypted data without decrypting it, preserving data privacy and security during processing in cloud environments.

10. Cloud Provider Security Services:

- **AWS Key Management Service (KMS), Azure Key Vault**: Cloud providers offer key management services for encrypting data, managing cryptographic keys, and enforcing access controls within their cloud platforms.

- These existing systems and technologies demonstrate the diverse array of tools and approaches available for securing data storage and sharing in cloud environments, catering to different security requirements, compliance needs, and industry standards. Organizations can leverage these systems, integrate them into their security frameworks, and implement best practices to enhance data protection in the cloud.

Chapter 3

PROPOSED SYSTEM

It represents a sharing environment where the data owners need to share the organization's valuable data to the cloud platform due to the limited storage and computational capacity of the enterprises and the multiple benefits of clouds .The cloud data is shared with multiple users as per different requirements for its utility purpose .Data leakage or loss may induce a severe threat to the organization's confidentiality.

Data Encryption:

- Use strong encryption algorithms such as AES (Advanced Encryption Standard) with key sizes of at least 256 bits to encrypt data before storing it in the cloud.
- Implement end-to-end encryption to ensure data remains encrypted during transmission and storage, and only authorized users possess the decryption keys.

Access Control:

- Utilize access control mechanisms to regulate who can access, modify, or delete data within the cloud environment.
- Implement role-based access control (RBAC) to assign permissions based on users' roles and responsibilities, ensuring least privilege access.

Data Masking and Anonymization:

- Apply data masking and anonymization techniques to protect sensitive information by replacing original data with fictitious but realistic data during storage and sharing processes.

Secure Authentication and Authorization:

- Use multi-factor authentication (MFA) to verify users' identities before granting access to data in the cloud.

Data Integrity Verification:

- Implement mechanisms for data integrity verification, such as cryptographic hash functions, to detect any unauthorized alterations to data stored in the cloud.

Backup and Disaster Recovery:

- Implement regular backup strategies to create redundant copies of data stored in the cloud, ensuring data availability and resilience against data loss incidents.

Secure Data Sharing Protocols:

- Utilize secure data sharing protocols such as HTTPS, FTPS, or SFTP for transferring data between cloud environments and external parties.

Secure Authentication and Authorization:

- Use multi-factor authentication (MFA) to verify users' identities before granting access to data in the cloud.

Compliance and Auditing:

- Ensure compliance with relevant data protection regulations and industry standards (e.g., GDPR, HIPAA, ISO/IEC 27001) regarding data storage and sharing in cloud environments.

User Education and Awareness:

- Provide training and awareness programs for users and administrators on secure data storage and sharing practices, including recognizing phishing attempts, creating strong passwords, and securely handling sensitive data.

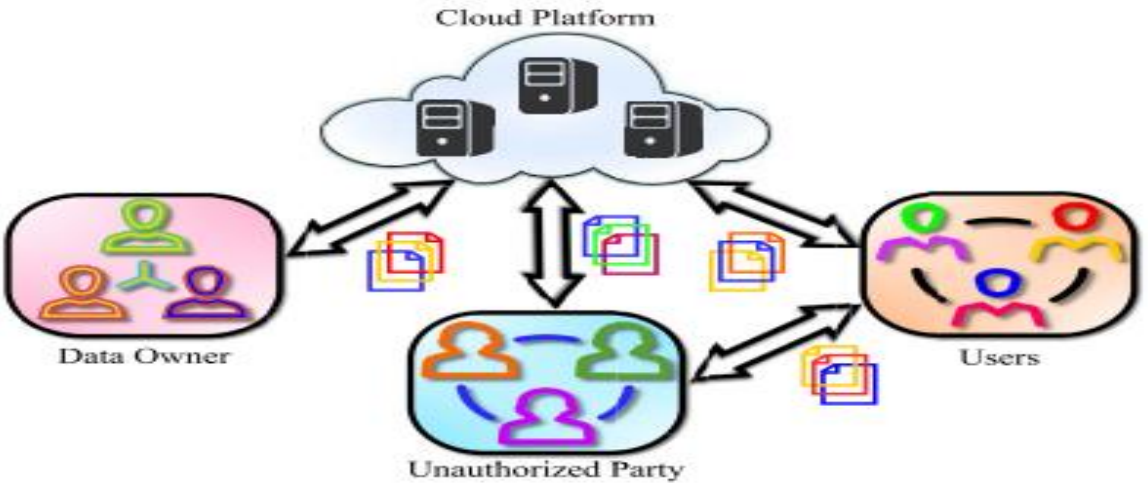

Fig 1.1 Block Diagram of sharing environment

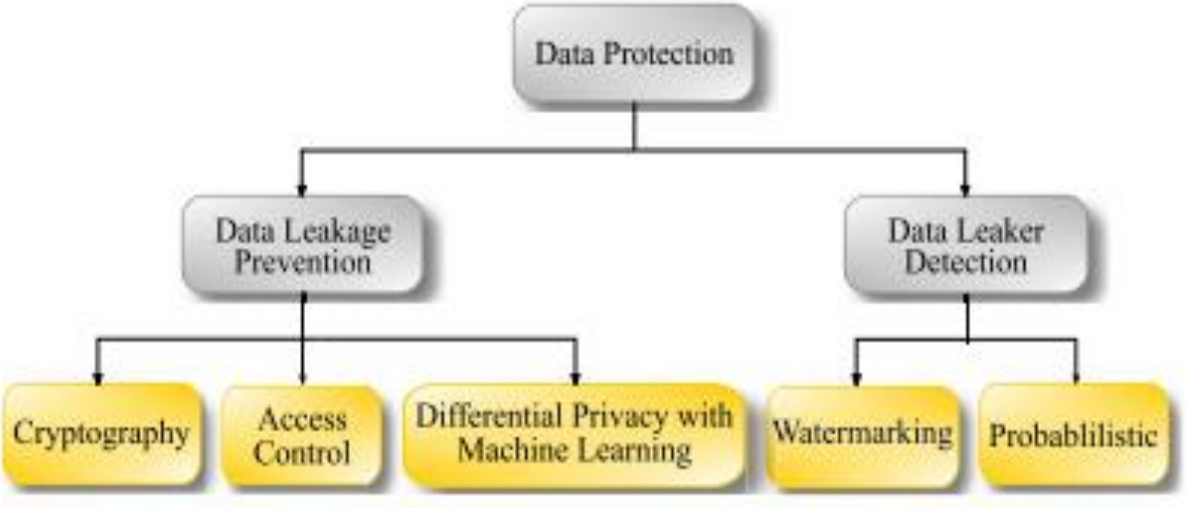

Fig 1.2 Major Classifications of Data Protection Techniques

Chapter 4

METHODOLOGY

The methodology for ensuring secure data storage and sharing techniques in cloud environments involves a systematic approach that encompasses various stages from planning to implementation and monitoring. Below is a detailed methodology outline for achieving secure data storage and sharing in cloud environments:

Risk Assessment and Requirement Analysis:

- Conduct a comprehensive risk assessment to identify potential threats, vulnerabilities, and compliance requirements related to data storage and sharing in the cloud.

Security Policy Development:

- Develop a robust security policy framework outlining guidelines, procedures, and controls for secure data storage and sharing practices in cloud environments.

Cloud Service Provider Evaluation:

- Evaluate and select a reputable cloud service provider (CSP) that complies with industry standards, offers strong security features, and provides transparency regarding data protection measures.

Data Classification and Encryption:

- Classify data based on sensitivity levels (e.g., confidential, sensitive, public) to determine appropriate encryption and protection mechanisms.

Backup and Disaster Recovery Planning:

- Develop and implement a comprehensive backup strategy to create redundant copies of data stored in the cloud, ensuring data availability and resilience against data loss incidents.

User Training and Awareness:

- Provide comprehensive training programs, workshops, and resources to educate users, administrators, and stakeholders on secure data storage and sharing practices in cloud environments.

Continuous Improvement and Compliance Monitoring:

- Conduct regular security assessments, vulnerability scans, and penetration testing to identify and remediate security gaps, misconfigurations, and emerging threats.

By following this methodology, organizations can establish a robust framework for secure data storage and sharing in cloud environments, mitigating risks, ensuring data confidentiality, integrity, and availability, and fostering a secure and compliant cloud computing environment.

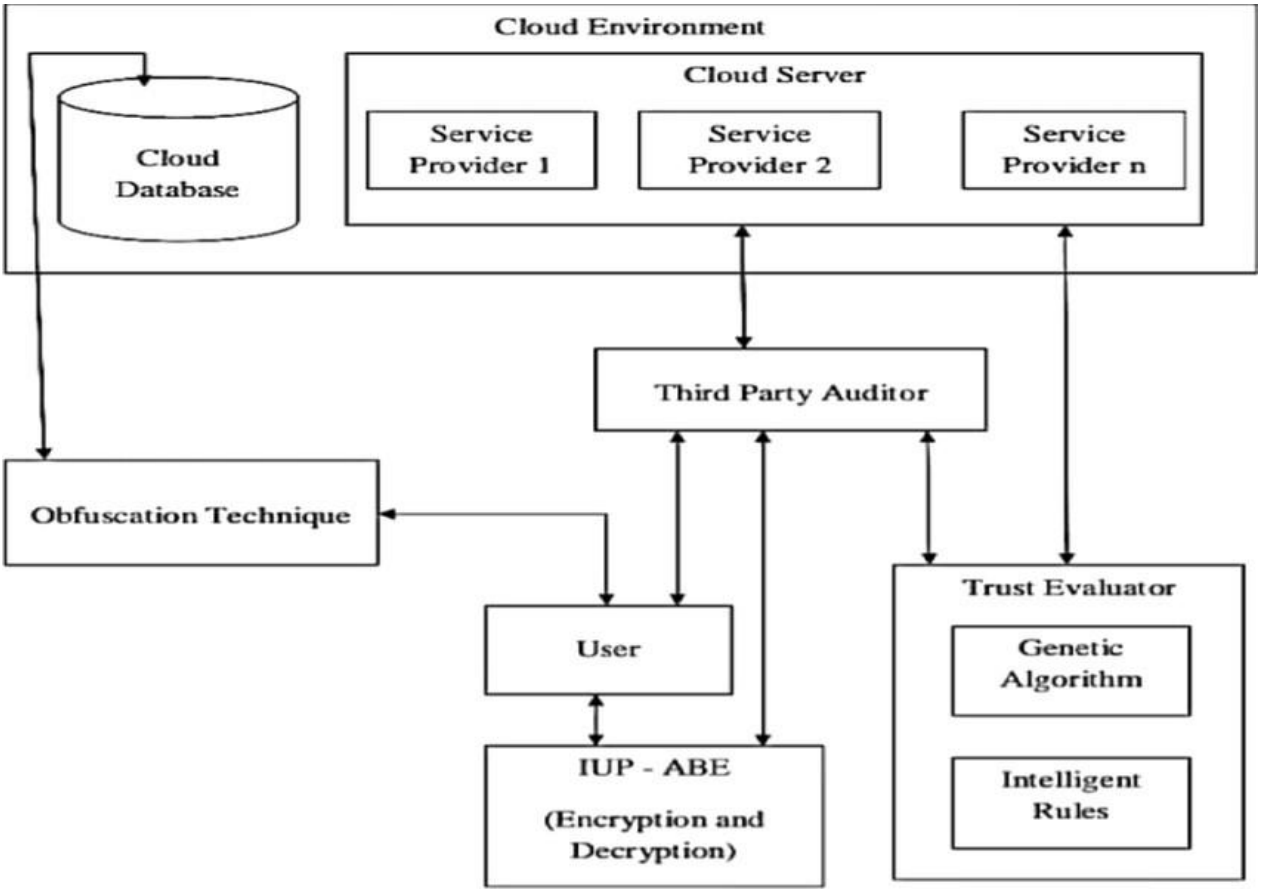

Fig 2.1 Methodology for Secure Data Sharing

Chapter 5

IMPLEMENTATION

1. **CRYPTOGRAPHY BASED MODELS**: The building block of the cryptography technique is demonstrated in Fig 3.1 Documents D = {D1, D2, . . . , Dn} are secured by encrypting it with the help of individual keys K = {K1,K2, . . . ,Kn} relatively and generated encrypted documents D E = {D E 1 , D E 2 , . . . , D E n } are passed to multiple stakeholders.

- The receiving party decrypts the acquired encrypted documents D E = {D E 1 , D E 2 , . . . , D E n } by using the shared keys K = {K1,K2, . . . ,Kn} and obtains the plain documents D = {D1, D2, . . . , Dn}. These documents are used by the receiving party after decrypting it.

Fig 3.1 Bird-eye view of Cryptography based model

2. **ACCESS CONTROL BASED MODELS**: The Access Control Mechanism ACM allows controlled exposure of the confidential data to the authorized entity based on data type, user type, user's privileges, and permissions .An Access Control Policy (ACP) is defined for data distribution among users

- ACP consists of a tuple (D, U, G) where D refers to a set of data objects D1, D2, . . . , Dn to be distributed, U denotes a set of users U1, U2, . . . , Um, and G is an expression or a set of expression that decide which Di can be accessed by which Uj or which Di can be allocated to which Uj or Uj is allowed to access which Di . ACP can vary depending upon the situations and applications.

- ACM provides the information flow control and is suitable for any organization if access rights and data classification are properly established.

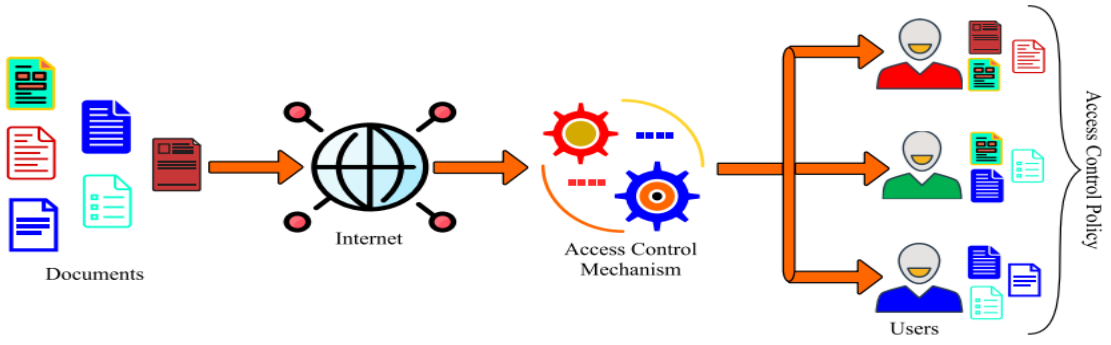

Fig 3.2 Schematic representation of access control based models

3. **DIFFERENTIAL PRIVACY WITH MACHINE LEARNING BASED MODELS**: Differential privacy with machine learning aims to protect sensitive information by making the outputs of different queries differing in at most one record indistinguishable. Differential privacy is a popular approach to privacy protection for machine learning algorithms on data sets.

- It controls how much information is disclosed about an individual's data through statistical analysis and computation. The lesser the value of , the more powerful is privacy protection .
- The main idea of Differential privacy in machine learning is to learn a simple rule automatically from the distributional information of the data set at hand without revealing too much about any single individual in the data set.

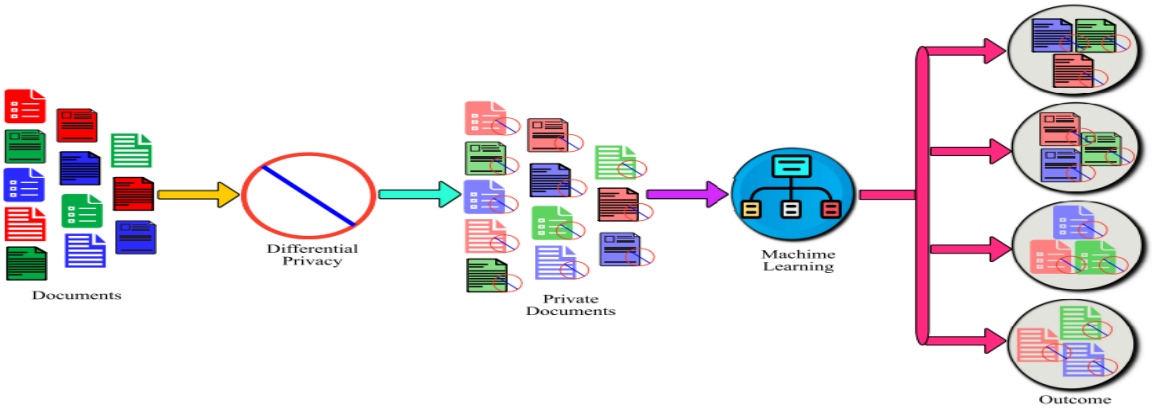

Fig 3.3 Standard model for differential privacy with machine learning.

4. **WATERMARKING BASED MODELS**: The figure depicts the basic components involved in the process of watermarking technique. Data D = {D1, D2, . . . , Dn} can be classified into various forms such as text, image, audio, video, relational, etc.

- A watermark Wm is implanted in Di using the watermark embedding process depending upon the category of Di and the watermark W ∗ m is extracted using the watermark extraction process as per the category of Di .

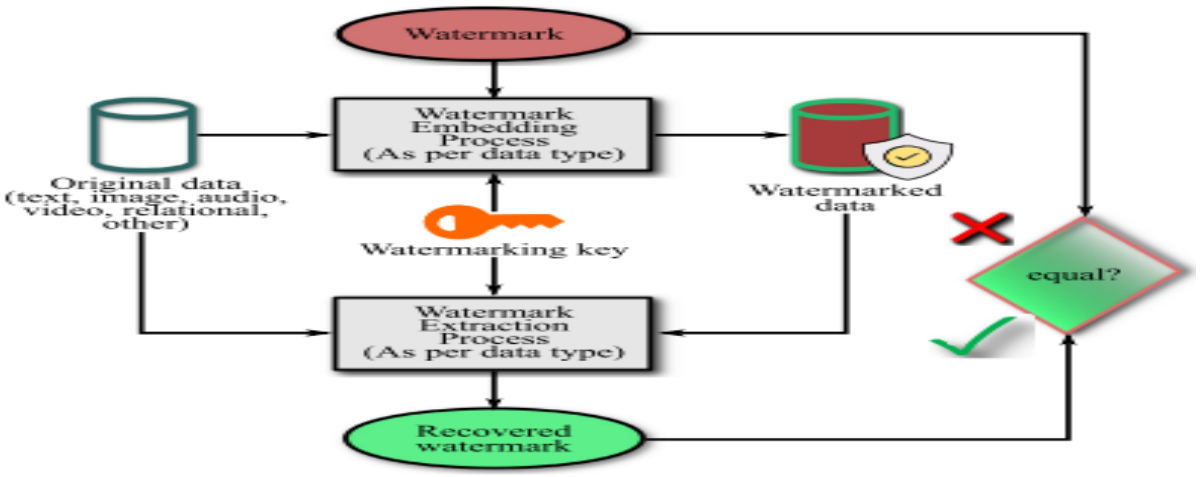

Fig 3.4 Key components of watermarking based models

Chapter 6

RESULT

The result of implementing secure data storage and sharing techniques in cloud environments is a strengthened security posture, reduced risk of data breaches, enhanced data protection, and improved compliance with regulatory requirements .Overall, the result of implementing secure data storage and sharing techniques in cloud environments is a robust security framework that protects data assets, mitigates risks, and builds trust with customers and stakeholders. It helps organizations leverage the benefits of cloud computing while maintaining a high level of data security and compliance.

CONCLUSION

In conclusion, secure data storage and sharing techniques in cloud environments are paramount in safeguarding sensitive information, maintaining data integrity, and ensuring compliance with regulatory standards. Through the implementation of robust security measures such as encryption, access control, authentication mechanisms, and secure data sharing protocols, organizations can mitigate risks associated with data breaches, unauthorized access, and data tampering.

By adopting a proactive approach to data security, including continuous monitoring, auditing, and user education, organizations can establish a strong security posture within their cloud environments. This not only protects valuable data assets but also builds trust with customers, partners, and stakeholders.

Furthermore, as cloud computing continues to evolve, it is crucial for organizations to stay abreast of emerging security trends, technologies, and best practices. This includes leveraging advancements in encryption algorithms, adopting cloud-native security solutions, and incorporating AI-driven security analytics for threat detection and response.

In essence, secure data storage and sharing in cloud environments require a holistic and multifaceted approach that combines technical controls, governance frameworks, and user awareness initiatives. By integrating these elements, organizations can harness the benefits of cloud computing while mitigating security risks and ensuring the confidentiality, integrity, and availability of their data assets.

REFERENCE

[1] A. K. Singh and I. Gupta, ‘‘Online information leaker identification scheme for secure data sharing,’’ Multimedia Tools Appl., vol. 79, no. 41, pp. 31165–31182, Nov. 2020

[2] E. Zaghloul, K. Zhou, and J. Ren, ‘‘P-MOD: Secure privilege-based multilevel organizational data-sharing in cloud computing,’’ IEEE Trans. Big Data, vol. 6, no. 4, pp. 804–815, Dec. 2020.

[3] I. Gupta and A. K. Singh, ‘‘GUIM-SMD: Guilty user identification model using summation matrix-based distribution,’’ IET Inf. Secur., vol. 14, no. 6, pp. 773–782, Nov. 2020.

[4] W. Shen, J. Qin, J. Yu, R. Hao, and J. Hu, ‘‘Enabling identity-based integrity auditing and data sharing with sensitive information hiding for secure cloud storage,’’ IEEE Trans. Inf. Forensics Security, vol. 14, no. 2, pp. 331–346, Feb. 2019.

[5] I. Gupta and A. K. Singh, ‘‘An integrated approach for data leaker detection in cloud environment,’’ J. Inf. Sci. Eng., vol. 36, no. 5, pp. 993–1005, Sep. 2020.

[6] R. Li, C. Shen, H. He, X. Gu, Z. Xu, and C.-Z. Xu, ‘‘A lightweight secure data sharing scheme for mobile cloud computing,’’ IEEE Trans. Cloud Comput., vol. 6, no. 2, pp. 344–357, Apr. 2018.

[7] I. Gupta, N. Singh, and A. K. Singh, ‘‘Layer-based privacy and security architecture for cloud data sharing,’’ J. Commun. Softw. Syst., vol. 15, no. 2, pp. 173–185, Apr. 2019.

[8] J. Li, S. Wang, Y. Li, H. Wang, H. Wang, H. Wang, J. Chen, and Z. You, ‘‘An efficient attribute-based encryption scheme with policy update and file update in cloud computing,’’ IEEE Trans. Ind. Informat., vol. 15, no. 12, pp. 6500–6509, Dec. 2019.

[9] C. Suisse. (2017). 2018 Data Center Market Drivers: Enablers Boosting Enterprise Cloud Growth. Accessed: May 19, 2019. [Online]. Available: https://cloudscene.com/news/2017/12/2018-data-center-predictions/

[10] I. Gupta and A. K. Singh, ‘‘A framework for malicious agent detection in cloud computing environment,’’ Int. J. Adv. Sci. Technol., vol. 135, pp. 49–62, Feb. 2020