International Journal of Innovative Trends In Engineering (IJITE)
Issue 114, Volume 74, Number 06, June 2022
e-ISSN: 2395-2946

Review Article

Research on Cloud Computing Data Security Using Data Classification Technique

Reetesh Rai[1], Dr. Ravindra Tiwari[2]

[1]*Research Scholar, LNCT University, Bhopal (M.P.), INDIA*
[2]*Guide, LNCT University, Bhopal (M.P.), INDIA*

ABSTRACT

To take advantage of the cloud's significant advantages of on-demand service, resource pooling, and rapid elasticity that helps to satisfy the demand for dynamically changing infrastructure without the burden of owning, managing, and maintaining it, organizations are now interested in moving their massive data and computations there. The security of the data in the cloud is a key challenge that needs to be concentrated on because the data is in a third party's premises and needs to be protected throughout its life cycle. One of the simplest methods for businesses to select and give relative values to the data they possess is data classification. Organizations can classify their stored data by sensitivity and business effect to assess the hazards related to the data using the data classification method. Instead of treating all data the same, organizations can manage their data in ways that represent its worth to them once the process is complete. More emphasis is placed on secure data storage as there is an increase in the number of personal and important data.

KEYWORDS

Cloud Computing; Data Security; Cloud Storage; Client Side Encryption, Cryptography, Multilevel Security.

1. INTRODUCTION

The ability to access highly scalable storage on demand and globally is made available to users via cloud storage. Controls including two-factor authentication, encryption, and other security measures have been put in place by CSPs to protect access to sensitive data in the cloud [5]. making it more challenging for attackers to obtain the data.

Although encryption is a popular and commonly used method of data protection, it is not completely reliable. Additionally, encrypting all cloud data is quite expensive to implement and requires a strong infrastructure in order to prevent illegal access [3]. As a result, it is not thought to be the greatest choice for CSPs. However, if security measures are tightened too much, consumers may stop using the system since the data becomes unusable. It is well known that not all of the data kept in cloud storage is secure or private. Some of the data require only minimal protection because they are less significant. Because consumers demand an equally efficient access to secured data as they do to plain text data, the majority of CSPs are unwilling to diminish the efficiency of accessing cloud storages. We anticipate the effort of protection based on a recognised level of data security selected by the users. Data protection security levels are an option that may be used to safeguard data stored in the cloud [9].

There are many ways to protect data, including grouping it into separate security groups with varying levels of protection. For instance, different levels of protection are applied to each of the many categories within the military services. Consider a scenario where top-secret assets are heavily shielded with multiple layers of protection before being accessible [13].

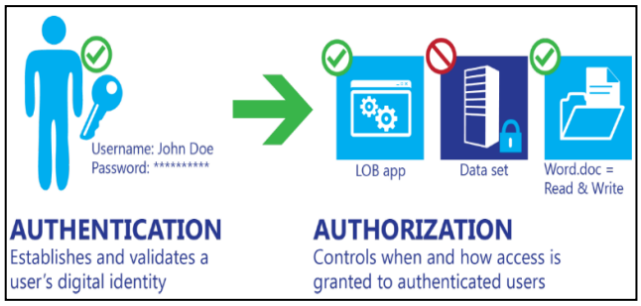

Fig. 1.1 Data Access Control

2. ROLES AND RESPONSIBILITIES IN CLOUD COMPUTING

Understanding the duties of businesses, cloud providers, and clients is crucial for authorization. It's critical to remember that cloud providers must meet any compliance needs a customer organisation may have in addition to having operational procedures in place to prevent unauthorised access to customer data [6]. Although cloud service providers can aid in risk management, clients must make sure that data classification management and enforcement are correctly handled to offer the required level of data management services.

Depending on the cloud service model in use, data classification responsibilities will change, as indicated in the accompanying figure. IaaS (infrastructure as a service), PaaS (platform as a service), and SaaS (software as a service) are

the three main cloud service paradigms (SaaS). Depending on how heavily a company relies on and what it expects from the cloud provider, different data classification procedures will be used [17].

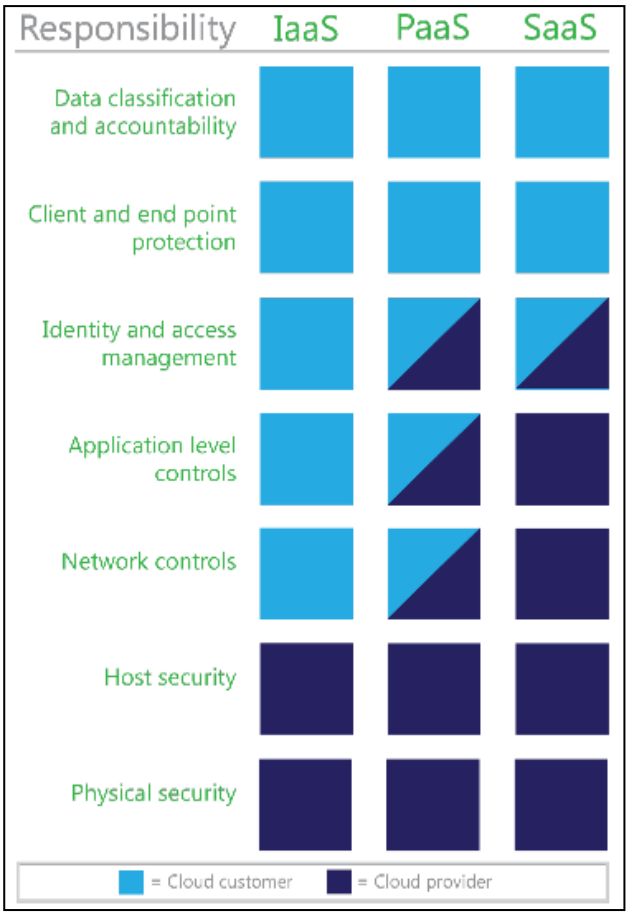

Fig 1.2 Cloud Computing Layer Responsibilities

Cloud providers should provide written guarantees to clients detailing how they will secure and uphold the privacy of customer data housed within their cloud, despite the fact that consumers are still in charge of classifying their data. These commitments should detail data use restrictions, privacy and security policies, and regulatory compliance. In order for customers to validate the efficacy of their cloud provider's practises, cloud providers should also make available certifications and audit reports that show compliance with standards like those set forth by the International Organization for Standardization (ISO) and controls like those outlined by the American Institute of CPAs Service Organization Controls (SOC1 and SOC2) [13]. Customers will be able to determine whether the cloud provider supports the data protection requirements imposed by their data classification with the aid of this information. Data migration shouldn't be done to a cloud provider that is unable to meet the customer's data protection requirements.

3. RELATED WORK

Previous studies on cloud storage have placed a strong emphasis on a variety of technical solutions to the aforementioned issues. Authentication, authorization, and encryption are the three procedures often used to evaluate access security solutions. Hardening passwords is one security measure that some people use [9]–[11]. Password security is ensured by creating strong passwords and keeping them from being stolen. Strong passwords must necessarily be lengthy, unpredictable, and tough to decipher but are frequently challenging to remember, according to researchers. According to Bang et al. [12], security is not only a technical problem but also a problem of user behaviour affecting, primarily, uneducated users. An authorization process ensures that a person has the authority to assess a given set of resources and access restrictions without knowing the identities of other users. Users might have access, but only if they are acting in accordance with their function or authority. In a multi-tenancy context, a publication proposed an authorization model appropriate for cloud services that enable path-based object hierarchies, federation, and hierarchical role-based access control (RBAC) [13]. These functions offer a practical authorisation service for clouds, particularly those that employ path-based patterns like REST APIs. Although high scalability is typically supported by authorisation, it is thought to improve scalability, which should allow for more precise control over the authorization information. There has been extensive research on applying encryption in a comprehensive manner, from data-in-transit through data-at-rest. designed a symmetric, asymmetric, and cloud-based encrypted storage system [14–15]. Applying encryption methods to secure sensitive data is a common practise. Although encryption has always been regarded as the highest level of security, there are a number of challenges involved. Transferring the data files locally and decrypting them is how traditional encryption is carried out. Early studies on the use of symmetric encryption algorithms that assure secrecy, integrity, and verifiability without using a lot of resources led to the creation of the cryptographic cloud storage system known as CS2 [14].

4. SECURITY THREATS

The service of cloud storage has advantages as well as disadvantages. Although it has flaws, users have never been deterred from using it to their advantage because of its functionality and adaptability. Data owners who use the cloud are worried about how safe and protected their data is there. Users no longer have control over the security of their data once a cloud model is adopted. In fact, users share resources with other users in the majority of well-known cloud storage systems. Security risks are a potential point of failure that could compromise security and harm a user or organisation. These dangers have the potential to have negative effects. An organisation may be under attack intentionally or unintentionally, from within or beyond. Numerous security threats are present in the cloud, according to earlier studies. In this part [2]–[6], we'll examine security risks associated with cloud storage.

5. DATA CLASSIFICATION IN DETERMINING SECURITY LEVELS OF PROTECTION

In a multi-tenant environment like the cloud, resources are shared. Threats might come from both inside and outside the shared environment. Sensitive data appears to be at risk when stored in shared cloud storage, though. Data privacy, loss, or leakage and being unavailable for access, whether unintentional or the result of a deliberate hacker assault, would constitute a serious breach of confidentiality, integrity, and availability. It is well known that not all of the

data kept in cloud storage is secure and private. Some require only minimal security since they are less significant. Because consumers demand an equally efficient access to secured data as they do to plain text data, the majority of CSPs are unwilling to diminish the efficiency of accessing cloud storages. We place a strong emphasis on protection based on a recognised security classification of user-determined data.

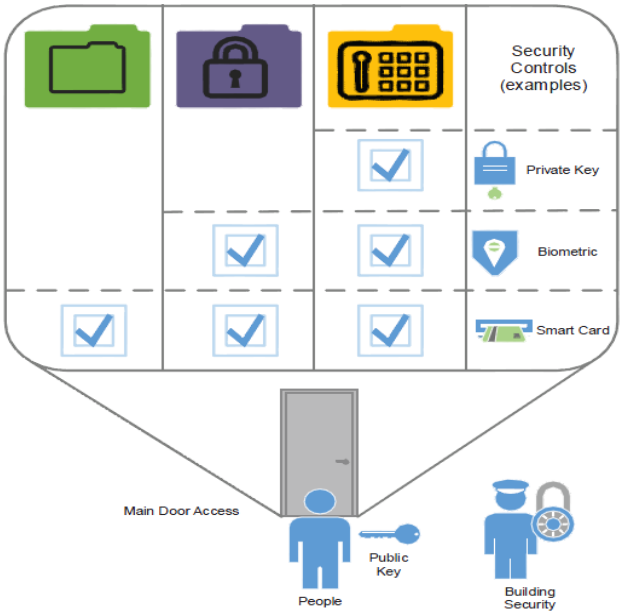

Fig. 1.3 Protection Levels

There are many techniques to protect data, including grouping it into separate security groups with varying levels of protection as depicted in the above image. Security protection is managed and organised into levels and categories for the most effective and efficient use. This process is known as security classification. The implementation of data protection is made simpler by a well-planned security classification scheme. In terms of risk management, legal discovery, and compliance, this can be particularly significant. Different data classifications in cloud storage will have varying degrees of sensitivity to sensitive information depending on the security level of protection assigned to them.

6. SECURITY PROTECTION LEVELS IN CLOUD STORAGE

Table 1.1 Security Protection Levels

Security Levels	Auth-entication	Authorization	Encryption
Protected	Single Factor	Administrator	SSL-128 bit
Sensitive	Multi-Factor	Administrator Secure Data Access Sharing	SSL-128/256 bit AES- 128
Top Secret	Multi-Factor	Super Admin Secure Data Access Sharing	SSL-128/256 bit AES-256 SHA-256

In this framework, we propose three levels of security classifications: protected, sensitive and top secret. In table above, the security protection levels in cloud storage is briefly shown. These security protections for protected and sensitive levels are based on existing control and measure by some known cloud storage providers.

i. Protected (Single Factor Authentication)

Protected level involves security protection for data that is for public or free distribution. Usually this includes data and that are not critical to user needs. This classification can also include data that has deliberately been shared to the public for use, such as marketing material. This level of protection is provided by most cloud storage provider in the market.

Single factor authentication usually involves single layer of security access such as password protected.

a. Authorization

A user is usually Administrators for their own data on cloud storage with privileges to create, edit and delete it.

b. Encrypted at Rest and In Transit

A normal encryption method in a cloud storage involve protecting data in transit using Secure Sockets Layer (SSL)/Transport Layer Security (TLS) for data transfer to create a secure tunnel protected by 128/256-bit SSL security.

ii. Sensitive (Multi Factor Authentication)

Sensitive level refers to security protection for information deemed to be of medium sensitivity, such as information that would not significantly harm the user in the event of loss or destruction. Data for private viewing are typically included in this classification. Corporate data may fall under this category because sensitive data is typically defined as information that is routinely viewed or used on a daily basis. utilising several forms of authentication, such as two-step verification or password re-entry Some CSPs have added password protection as the first tier of authentication and another layer of authentication using security codes sent to the registered mobile phone or a mobile app.

a. Authorization

A user is usually Administrators for their own data on cloud storage with privileges to create, edit and delete it.

b. Encrypted at Rest and in Transit

Secure Sockets Layer (SSL)/Transport Layer Security (TLS) for data transfer creates a secure tunnel secured by 128/256-bit or greater Advanced Encryption Standard (AES) encryption as part of a typical encryption mechanism in a cloud storage. It is secured once it is in the cloud storage using 128-bit AES encryption at rest.

c. Top Secret (Multi Factor Authentication)

Top secret level involves security protection for data that is classified as confidential or restricted including data that can be catastrophic to one or more user if com-promised or lost such as personal data, including personally identifiable information such as Social Security or national identification numbers (passport numbers etc.), specific intellectual property, legal data, authentication data (private cryptography keys, username password pairs, or other identification sequences such as private biometric key files).

Multi-factor authentication such as two-step verification or re-entering password. Some CSP has introduced security codes sent to the registered mobile number or using a mobile app.

d. Authorization

In a top-secret level, a user is a Super Admin with privileges to create, edit and delete data and but with highest level of access.

e. Encrypted at rest, in process, and in transit

A top-secret encryption method in a cloud storage involves protecting data in transit using Secure Sockets Layer (SSL)/Transport Layer Security (TLS) for data transfer to create a secure tunnel protected by 128/256-bit or higher Advanced Encryption Standard (AES) encryption. Once it reaches the cloud storage, it is protected using 128/256-bit AES encryption at rest. The data in process (in-use) is protected using 128/256-bit AES encryption or SHA.

7. CONCLUSION AND FUTURE WORK

Users share resources to store their data online in a shared environment called the cloud. In the cloud, security threats are prevalent. Password cracking, uneven encryption use, malware, hardware failure, DDoS, and Man in the Middle attacks are some of the dangers. To combat these dangers, CSPs have implemented mandatory security measures and controls. Although cloud storage contains numerous built-in security mechanisms to secure data, a solid framework with security categories for cloud storage data hasn't been fully investigated yet. Total encryption is one of the most tempting alternatives, but it is rarely used because it requires a substantial and expensive infrastructure. As a result, we suggest a framework for cloud storage security that bases measures and controls on security categories. As a recommended security classifications guide, it is important to note the protection levels of protected, sensitive, and top secret. With the offered technical security solutions, risk is also anticipated to be reduced and mitigated.

REFERENCES

[1] Gartner, press release from 2012 titled "Newsroom: Consumers Will Store More Than a Third of Their Digital Content in the Cloud by 2016."

[2] The CSA published "Top Threats to Cloud Computing V1.0" in 2010.

[3] The Cloud Computing Association, "Cloud Computing Vulnerability Incidents: A Statistical Overview," 2013.

[4] Emerging Cyber Threats Report 2014, GTISC and GTRI, 2013.

[5] F. Sabahi, "Cloud computing security challenges and responses," 2011 IEEE 3rd International Conference on Communications Softw. Networks, pages 245-249, May 2011.

[6] S. Haider and F. Bashir Shaikh, "Security Threats in Cloud Computing," 6th International Conference on Information Technology Security, Abu Dhabi, United Arab Emirates, no. December 2011, pp. 11–14.

[7] CISO Perspectives: Data classification, Microsoft, 2007. Microsoft Trusted Computing Doc., 2014, pp. 1–5.

[8] Frank Simorjay, "Data classification for cloud readiness," Microsoft Trust.

[9] M. Weir, S. Aggarwal, B. De Medeiros, and B. Glodek "Password cracking using probabilistic context-free grammars," Proceedings - IEEE Symposium on Security and Privacy, 2009, pp. 391-405.

[10] P. G. Kelley, S. Komanduri, M. L. Mazurek, R. Shay, T. Vidas, L. Bauer, N. Christin, L. F. Cranor, and J. López, "Guess again (and again and again): Measuring password strength by simulating password cracking algorithms," in Proceedings - IEEE Symposium on Security and Privacy, 2012, pp. 523-537.

[11] R. Zhao and C. Yue, "Toward a safe and practical cloud-based password manager for web browsers," Comput. Secur., vol. 46, no. 10, october 2014, pp. 32–47.

[12] "Improving information security management: An investigation of ID-password usage and a novel login vulnerability measure," International Journal of Information Management, vol. 32, no. 5, Oct. 2012, pp. 409–418.

[13] "Toward a Multi-Tenancy Authorization System for Cloud Services," no. December 2010.

[14] J. M. A. Calero, N. Edwards, J. Kirschnik, L. Wilcock, and M. Wray, "CS2_: A Searchable Cryptographic Cloud Storage System," S. Kamara, C. Papamanthou, and T. Roeder, 2011, pp. 1–25.

[15] H. M. Al-sabri and S. M. Al-saleem, Building a Cloud Storage Encryption (CSE) Architecture for Enhancing Cloud Security, vol. 10, no. 2, pp. 259-266, 2013.

[16] "K2C: Cryptographic cloud storage with lazy revocation and anonymous access," Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Tele-communications Engineering, 2012, vol. 96 LNICST, pp. 59–76.

[17] P. Chen and R. Zhang, "A Dynamic Cryptographic Access Control Scheme in Cloud Storage Services," International Journal of Information and Process Management, vol. 4, no. 1, January 2013, pp. 104–111.

[18] D. Koo, J. Hur, and H. Yoon, Secure and effective data retrieval over encrypted data using attribute-based encryption in cloud storage, Comput. Electr. Eng., vol. 39, no. 1, Jan. 2013, pp. 34–46.

[19] R. V. Agalya and K. K. Lekshmi, "A Verifiable Cloud Storage Using Attribute Based Encryption and Outsourced Decryption with Recoverability," vol. 3, no. 10, 2014,