ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 11, November 2017

Survey on File Security Using Encryption Technique over Public Cloud Environment

Ruchita Datta, Prof. Saurabh Sharma

Research Scholar, Dept. of Computer Science & Engg, Gyan Ganga College of Technology, Jabalpur, India

Assistant Professor, Dept. of Computer Science & Engg, Gyan Ganga College of Technology, Jabalpur, India

ABSTRACT: In the world of computing, security and privacy issues are a major concern and cloud computing is no exception to these issues. In this paper we outline a security protocol called as Security as a Service (SasS). We provide a mechanism for achieving maximum security by leveraging the capabilities of a processor called a cryptographic coprocessor. Further we enhance the security of the encrypted data by distributing the data within the cloud, i.e. we divide the user data into pieces called as chunks. SasS protocol gives the user a chance to define the security of their data, by leaving the option of dividing the data into chunks in the user's hand. Based on the user requirement data will be made into chunks. Each chunk after encryption will be stored in a separate database. In this way we provide the maximum security to a user data. To our best knowledge, for the first time security is offered as a service to the user.

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

I. INTRODUCTION

The cloud storage provides the facility for user requiring mainly highly scalable storage on demand and accessible globally. CSPs have been implementing controls to secure access to sensitive data in the cloud such as two-factor authentication, encryption etc [5]. making access to the data more difficult for attackers.

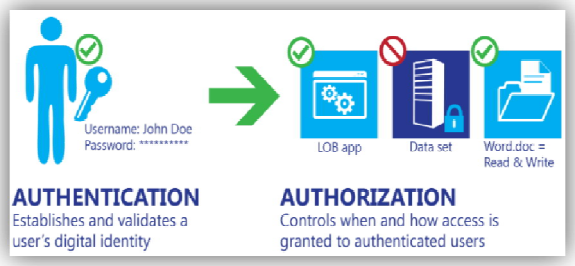

Fig. 1.1 Data Access Control

Encryption is an effective and widely known as the primary solution to protect data but it is not fool-proof. Additionally, to encrypt the whole data on cloud in order to protect against unauthorized accessed will need a robust infrastructure and is greatly expensive to be enforced [3]. Therefore, it has not been consider as the best option for CSPs. Then again, an increase in security measures affects the usability of the data and therefore causing the system to be shunned by users. It is known that not all data stored in cloud storage is private or confidential. Some of the data is less important and therefore need basic protection. Most CSPs are unwilling to reduce the efficiency of accessing into cloud storages because users expect an equally efficient access into a secured data as the plain text ones. We foresee the effort of protection based on an acknowledged security level of data determined by the users. Security levels for data protection can be applied as an option to protect data in cloud storage [9]. There are various ways of protecting a data

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 11, November 2017

such as categorizing it into several security groups having different level of protection mechanism. For an example, in the military services, several categorizations are for each category, different level of protection is applied. Imagine top secret assets are protected in-depth with multilayer of shields before the asset can be accessed [13].

II. ROLES AND RESPONSIBILITIES IN CLOUD COMPUTING

Authorization requires an essential understanding of the roles and responsibilities of organizations, cloud providers, and customers. Cloud providers must have operational practices in place to prevent unauthorized access to customer data; it's also important to note that any compliance requirements a customer organization has must also be supported by the provider [6]. Although cloud providers can help manage risks, customers need to ensure that data classification management and enforcement is properly implemented to provide the appropriate level of data management services.
Data classification responsibilities will vary based on which cloud service model is in place, as shown in the following figure. The three primary cloud service models are infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). Implementation of data classification mechanisms will also vary based on the reliance on and expectations of the cloud provider [17].

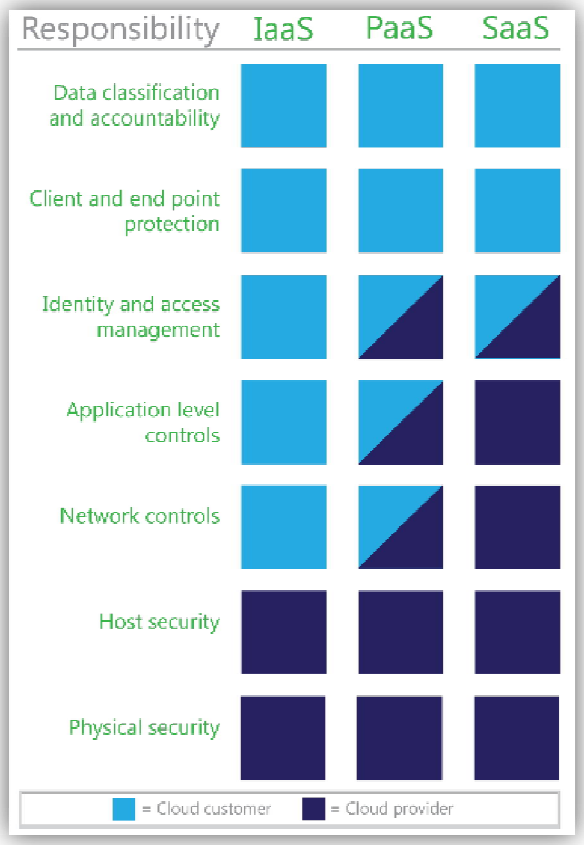

Fig 1.2 Cloud Computing Layer Responsibilities

Although customers are responsible for classifying their data, cloud providers should make written commitments to customers about how they will secure and maintain the privacy of the customer data stored within their cloud. These

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 11, November 2017

commitments should include information about privacy and security practices, data use limitations, and regulatory compliance. In addition, cloud providers should make certifications and audit reports that demonstrate compliance with standards such as the International Organization for Standardization (ISO) and controls such as the American Institute of CPAs Service Organization Controls (SOC1 and SOC2) available so customers can verify the effectiveness of their cloud provider's practices [13]. Having this information will help customers understand whether the cloud provider supports the data protection requirements mandated by their data classification. Customers should not migrate data to a cloud provider that cannot address their data protection needs.

III. RELATED WORK

Previous researches on cloud storage have emphasis on a wide range of technical approaches over the fore mentioned concerns. Access security measures are generally considered in three steps: Authentication, Authorization and Encryption.

Some security measure includes effort to secure access based on hardening passwords [9]–[11]. Generating strong passwords and protecting them from getting stolen guarantees a password security. Researchers have established that strong passwords are necessarily long, random and hard to crack but often difficult to remember. Bang et al. suggests that security is not just a technical issue but also a behavioural issue involving users, mostly untrained ones [12]. An authorization process ensures that a person has the right to assess a certain re-sources and limits of the access unknowing of other user information. Users may have access but have a specific role or authority to do something within their scope. A paper suggested an authorization model suitable for cloud services that support hierarchical role-based access control (RBAC), path-based object hierarchies and federation [13] in multi-tenancy environment. These features provide a convenient authorization service for cloud, especially those using path-based patterns such as REST APIs. Although authorization usually supports high scalability, it is believed to improve scalability and this would hopefully enable more fine grained control on the authorization information. A comprehensive approach using encryption ranging from data-in-transit to data-at-rest have been researched widely. Mostly developed a cryptographic cloud storage system; symmetric [14], [15] and asymmetric [16]–[19]. It is a standard approach to apply encryption techniques into sensitive data to secure it. Encryption has always been seen as the ultimate security measure but it also comes with a set of difficulties. Traditional encryption is done by transferring the data files locally and decrypting it. A cryptographic cloud storage system called CS2 was amongst early research done on applying symmetric encryption techniques that ensures confidentiality, integrity and verifiability without being resource hungry [14].

IV. SECURITY THREATS

Cloud storage is a service that comprises of benefits and also challenges. It inherent vulnerabilities, but these have never discourage users from taking advantage of its functionality and flexibilities. Cloud users are data owners that have concerns whether their data are secured and protected in the cloud. With the adoption of a cloud model, users lose control over data security. In fact, in most known cloud storage, users are sharing the resources with other users. Security threats are a possible vulnerability that may breach security and cause harm to a user or organization. These threats are potential in causing adverse impact. A threat may be happening from inside or outside of an organization or either intentional or accidental. In previous researches, it is shown many security threats are happening in the cloud. We will review security threats happening in cloud storage in this section [2]–[6].

V. DATA CLASSIFICATION IN DETERMINING SECURITY LEVELS OF PROTECTION

The cloud is a multi-tenant environment, where resources are shared. Threats can happen from anywhere; inside the shared environment or from outside of it. However, placing sensitive data in shared cloud storage is apparently risky. Accidental or due to a malicious hacker attack, data privacy, loss or leakage and unavailable for access would be a major security violation involving confidentiality, integrity and availability.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 11, November 2017

It is known that not all data stored in cloud storage are private and confidential. Some are less important and therefore need basic protection. Most CSPs are unwilling to reduce the efficiency of accessing into cloud storages because users expect an equally efficient access into a secured data as the plain text ones. We are emphasizing on protection based on an acknowledged security classification of data determined by the users.

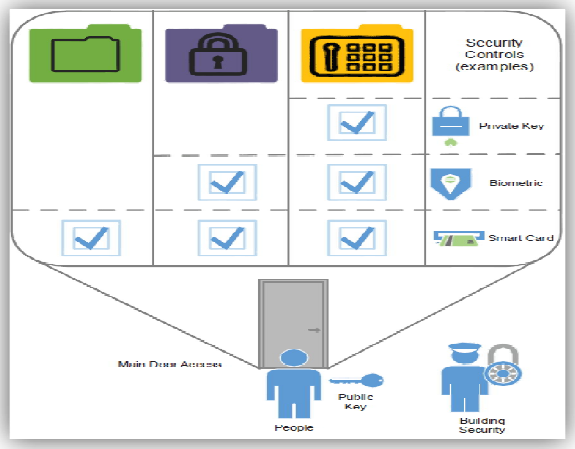

Fig. 1.3 Protection Levels

There are various ways of protecting a data such as categorizing it into several security groups having different level of protection mechanism as shown in figure above. Security classification is known as the process of managing and organising security protection into levels and categories for its most effective and efficient application. A well-planned security classification system makes data protection easier to implement. This can be of particular importance for risk management, legal discovery, and compliance. Assigning a security level of protection to different data classification in cloud storage will give different level of sensitivity to classified information.

VI. SECURITY PROTECTION LEVELS IN CLOUD STORAGE

Data Chunks	Encryption
Chunks 1	AES 128
Chunks 2	AES 256
Chunks 3	TRIPLE DES

Table 1.1 Security Protection Levels

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.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 11, November 2017

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.

ii. Sensitive
Sensitive level involves security protection for data that is classified as being of medium sensitivity including data that would not have a severe impact on the user if lost or destroyed. Generally, this classification includes data for non-public view. This classification may include corporate data as most data that are accessed frequently or in daily use can be classified as sensitive.

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 or higher Advanced Encryption Standard (AES) encryption. Once it reaches the cloud storage, it is protected using 128-bit AES encryption at rest.

iii. 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.

b. 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.

c. Encrypted at rest, in process, and in transit
A top secret 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 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.

VII. CONCLUSION AND FUTURE WORK

The cloud is a mutual environment, where users are sharing the resources to store their data online. Security threats are happening widely in the cloud. The threats includes, password cracking, inconsistent use of encryption, malware, hardware failure, DDoS, and Man in the middle attack. CSPs have introduced obligatory security measure and controls in undertaking these threats. Although there are many security controls built-in to protect data stored in cloud storage but a reliable framework that have security classifications for data stored in cloud storage has less been explored yet. Some solutions like total encryption is known as one of the appealing solution but it is barely implemented due to the need of a robust and costly infrastructure. Therefore, we propose a cloud storage security framework whereby the measure and controls are done based on security classifications. The suggested security classification of protection

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 11, November 2017

levels: protected, sensitive and top secret are worth noting as a recommended security classifications guide. It is also expected to help reduce and mitigate risk with the suggested technical security solutions.

REFERENCES

[1] Gartner, "Newsroom: Consumers Will Store More Than a Third of Their Digital Content in the Cloud by 2016," Press Release, 2012.
[2] CSA, "Top Threats to Cloud Computing V1.0," 2010.
[3] CSA, "Cloud Computing Vulnerability Incidents_: A Statistical Overview," 2013.
[4] GTISC and GTRI, "Emerging Cyber Threats Report 2014," 2013.
[5] F. Sabahi, "Cloud computing security threats and responses," 2011 IEEE 3rd Int. Conf. Commun. Softw. Networks, pp. 245–249, May 2011.
[6] F. Bashir Shaikh and S. Haider, "Security Threats in Cloud Computing," 6th Int. Conf. Internet Technol. Secur. Trans. Abu Dhabi, UAE, no. December, pp. 11–14, 2011.
[7] Microsoft, "CISO Perspectives: Data classification," Microsoft Trust. Comput. Doc., pp. 1–5, 2014.
[8] Frank Simorjay, "Data classification for cloud readiness," Microsoft Trust. Comput. Doc., pp. 1 – 19, 2014.
[9] M. Weir, S. Aggarwal, B. De Medeiros, and B. Glodek, "Password cracking using probabilistic context-free grammars," in 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 passwordcracking
algorithms," in Proceedings - IEEE Symposium on Security and Privacy, 2012, pp. 523–537.
[11] R. Zhao and C. Yue, "Toward a secure and usable cloud-based password manager for web browsers," Comput. Secur., vol. 46, pp. 32–47, Oct. 2014.
[12] Y. Bang, D.-J. Lee, Y.-S. Bae, and J.-H. Ahn, "Improving information security management: An analysis of ID–password usage and a new login vulnerability measure," Int. J. Inf. Manage., vol. 32, no. 5, pp. 409–418, Oct. 2012.
[13] J. M. A. Calero, N. Edwards, J. Kirschnik, L. Wilcock, and M. Wray, "Toward a Multi-Tenancy Authorization System for Cloud Services," no. December, 2010.
[14] S. Kamara, C. Papamanthou, and T. Roeder, "CS2_: A Searchable Cryptographic Cloud Storage System," pp. 1–25, 2011.
[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] S. Zarandioon, D. Yao, and V. Ganapathy, "K2C: Cryptographic cloud storage with lazy revocation and anonymous access," in Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 2012, vol. 96 LNICST, pp. 59–76.
[17] R. Zhang and P. Chen, "A Dynamic Cryptographic Access Control Scheme in Cloud Storage Services," Int. J. Inf. Process. Manag., vol. 4, no. 1, pp. 104–111, Jan. 2013.
[18] D. Koo, J. Hur, and H. Yoon, "Secure and efficient data retrieval over encrypted data using attribute-based encryption in cloud storage," Comput. Electr. Eng., vol. 39, no. 1, pp. 34–46, Jan. 2013.
[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