Data Security in Cloud Computing using Encryption and Obfuscation Techniques

Thesis · October 2017

DOI: 10.13140/RG.2.2.30452.40323

2 authors:

Krunal Suthar
Sankalchand Patel College of Engineering
10 PUBLICATIONS **29** CITATIONS
SEE PROFILE

Jayeshkumar Madhubhai Patel
Ganpat University
96 PUBLICATIONS **216** CITATIONS
SEE PROFILE

CHAPTER 1

Introduction

1.1 Basics

1.2 Cloud Computing

1.2.1 Cloud Services

1.2.2 Cloud deployment Models

1.2.3 Cloud Life cycles

1.3 Data Obfuscation

1.3.1 Basics

1.3.2 Obfuscation Techniques

1.4 Cryptography

1.1 Basics

Now a day, everyone is connected with this digital world by one or another way and this is the main reason behind the growth of information technology. The main factor behind this is the user friendly environment that is accessible from anywhere and anytime. The internet provides facility for various groups of people such as businessmen, researchers, students etc. to complete their works by giving lots of options to fulfill their goals.

Lots of users connect themselves with internet and use IT infrastructure to complete their day to day requirements. As the demand of internet is increasing, the service provided such as Software, Platform, Database services, Storage services etc. through internet also gradually increases. Here the important terms cloud computing comes into existence which provides huge amount of different services to its users via network. As it provides 'Pay as you Go' fundamental user can get maximum benefits by using this service for cheaper cost.

1.2 Cloud Computing

Cloud is an Internet-based computing technology, where shared resources such as software, platform, storage and information are provided to customers on demand. Cloud Computing is a computing platform for sharing resources that include infrastructures, software, applications, and business processes. Cloud Computing is a virtual pool of computing resources. It provides computing resources in the pool for users through internet. Cloud computing as an emerging computing paradigm aims to share storage, computation and services transparently among massive users. Current Cloud computing systems poses serious limitation in protecting users' data confidentiality. Since users' sensitive data is presented in unencrypted forms to remote machines owned and operated by third party service providers, the risks of unauthorized disclosure of the users' sensitive data by service providers may be quite high. There are many techniques for protecting users' data from outside attackers. An

approach is presented to protecting the confidentiality of users' data from service providers, and ensures service providers cannot collect users' confidential data while the data is processed and stored in Cloud computing systems. Cloud computing systems provide various internet based data storage and services. Due to its many major benefits, including cost effectiveness and high scalability and flexibility, Cloud computing is gaining significant momentum recently as a new paradigm of distributed computing for various applications, especially for business applications along with the rapid growth of the Internet. With the rise of the era of "Cloud computing", concerns about "Internet Security" continue to increase. How will customers of the "Cloud" know that their information will be available to them, as well as secure and safe from others?

The term "Cloud" in Cloud computing is the communication network or a network which is Combined with computing infrastructure. Cloud computing system is accessed using network which provides software, hardware, processing power etc. to the user when demand is generated. Cloud Computing is a virtual pool of computing resources which provides the pool to users through internet.

Cloud Computing [1] provides various services to user by creating group of clusters and grids of computers. The main goal behind this is to provide services in virtualized manner to reduce burden of user to maintain everything by itself. It also refers to the web-based computing which provides devices with shared pool of resources, information or software on demand and pay per-use basis. Instead of having local servers or own devices to manage applications, people use sharing computing resources model of Cloud.

The Cloud computing provides environment in which user can have its own virtual infrastructure using which they can perform tasks without depending on geographical boundary. Because of the flexible environment and cheaper cost, people are attracted towards the use of Cloud services that may be related to Platform, software or

infrastructure. Based on the usage of Cloud, there are three deployment models: Public Cloud, Private Cloud and Hybrid Cloud.

The Cloud computing provides a numerous advantages to its users but at the dark side it's also suffers from lots of issues like Integrity or Storage Correctness, Availability, Confidentiality and more. These issues make the adaption of cloud environment somewhat difficult for the users. Therefore lots of research is required in this direction to set a trust of Cloud user on Cloud service providers.

1.2.1 Cloud Services

Cloud provides four types of services based on different requirements of clients as shown in below figure.

Software-as-a-Service (SaaS): In software as a service, cloud service providers provide different software. It leads to better storage utilization of our workstation. Saas vendor provides best software infrastructure like software, network spaces and data center for best solution in developing industry. Examples of SaaS includes: Salesforce.com, Google Apps.

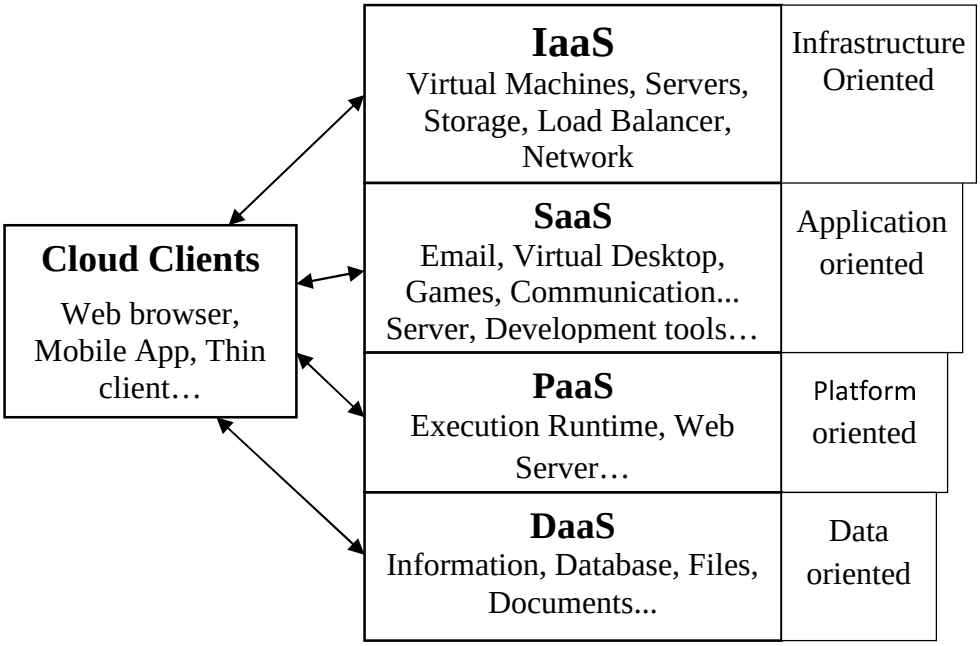

Figure 1.1 : Cloud services [22]

Platform as a Service (PaaS): It is the way to use and access service of software without downloading on user's premises or even no need to install it on local machine for any user whether its developer or any end user. It provides great level of platform integration for multitenant systems. When the users are not able to manage the network, servers, operating systems and storage, they opt Platform as a Service. Some examples of PaaS are Force.com, Google App Engine and Microsoft Azure. [22]

Infrastructure as a Service (IaaS): IAAS is a sharing multiple physical resources over network. Main purpose of IAAS is to provide rapid access for server, storage and network by applications and OS. Thus, it offers simple infrastructure on-demand services using Application Programming Interface (API).The user does not need to manage the primary hardware in the cloud infrastructure, but he can control server, application and OS. Some examples of IaaS are Amazon Elastic Cloud Computing (EC2) etc.

Database as a Service (DaaS): DaaS is about the storing of users important document files and other information. This also provides the services related to storing large amount of files which may be mine to fetch relevant information. The database is also an important part of these services which store users related information like personal information, credential information etc.

1.2.2 Cloud Models

Cloud provides three types of models: Public Cloud which is open for all; Private Cloud where access is only permitted to the user who are the user of that private area; Hybrid cloud which is performing compromise task of both types of services provided by public and private Cloud.

There are four deployment models [34] which are defined as below:

Private Cloud:

This structure is for any single organization whose employee internally uses it. Generally, this Cloud infrastructure is managed by organization itself or can take help from any third party.

Public Cloud:

The organization providing Cloud services by giving platform open for access to general public who can access it from anywhere and pay as per use.

Community Cloud:

This is cloud system used by the several communities together where all the members are having equal access to this infrastructure.

Hybrid Cloud:

Two or more of above cloud models jointly providing efficient services to client makes an hybrid infrastructure where some of the art may be restricted for general public and some parts are open to all for access.

1.2.3 Cloud Service Lifecycle:

The service life cycle [35] for Cloud consists of the following steps showing in figure:

1. Request Formulation: The user defines at design time the functional and nonfunctional SLA requirements for the requested Cloud service.

2. Discovery and Monitoring: Discovers the candidate service offers and stores their Monitored SLA metrics and pricing information in different data repositories.

3. Matchmaking**:** Selects the suitable Clouds for provisioning the requested service by matching the SLA requirements to the candidate computing and storage resources.

4. Deployment**:** Deploys the service components on the selected providers.

5. Execution: The service is executed and its status is continually monitored at the runtime.

6. Termination: The service can be terminated upon user request. (e.g., in case of repeated SLA violations).

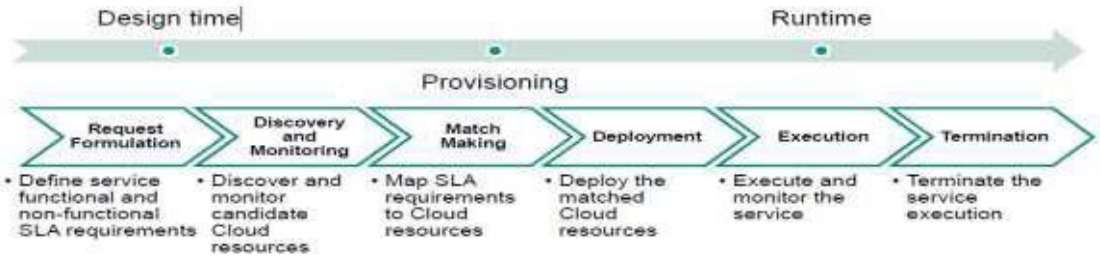

Figure 1.2: Cloud Service Lifecycle[36]

Advantages of Cloud Computing:-

- ✓ *Cost efficiency* – Cloud computing is best and low cost method for using software, platform and infrastructure services. It is based on 'pay as you go' so no need to pay extra money for it.

- ✓ *Almost Unlimited Storage* - Storing capacity of cloud storage is unlimited so there is no limitation to store the data.

- ✓ *Backup and Recovery*-In cloud computing it is easy to get back up and recover it.

- ✓ *Automatic Software Integration*-In the cloud computing software integration is typically something that occurs automatically. So user needs not to give extra effort to customize application as per his needs.

- ✓ *Easy Access to Information*- In cloud, once user is registered, then he can use from anywhere his data and no location limitation.

Disadvantages of Cloud Computing:-

There are some limitations in cloud computing which is given below.

- ✓ *Technical Issues*- technical issue of network access.

- ✓ *Security in the Cloud*-Security is main issue in cloud computing. In cloud computing so many users can access to use cloud storage. So users may face issues pertaining to security in terms of authentication, confidentiality and integrity.

- ✓ *Possible downtime*-Cloud computing makes the minor business dependent on the reliability of their Internet connection.

Purpose of data security is to hide sensitive information from out-siders and un authorized parties. This area of data security has gained more attention over the recent period of time due to the massive increase in data transfer rate.

1.3 Data Obfuscation

1.3.1 Basics

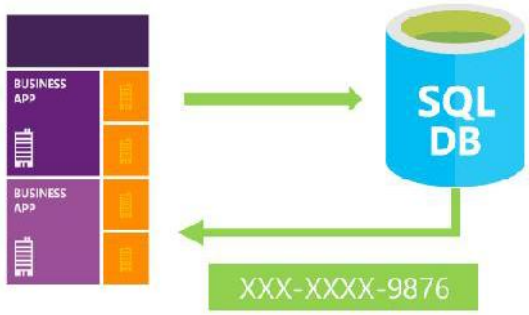

Figure 1.3 Obfuscation [30]

Using obfuscation the representation of the user data are changed .using a public, generally-understood, and (usually) low-overhead method for the purpose of allowing the data to survive intact and easily recoverable after some sort of transfer.

1.3.2 Obfuscation Techniques

Data Obfuscation techniques can be classified by a number of criteria:

- ✓ Usefulness – it's a measure about how much the obfuscated data are useful after conversion.

- ✓ Potency - measures about knowledge, effort and time required by unauthorized user to get the idea about the obfuscated details.

- ✓ Resiliency - measures how difficult for an attacker to create a program which unobfuscate the details. More resiliency increase the security of obfuscated construct towards automated unobfuscation.

- ✓ Cost - measures the time needed to create program which implement previous two methods for execution of the development/testing program e.g. method that requires large memory or more time having large cost.

Table 1.1 Obfuscation techniques [9][11]

Strength of Obfuscation Technique[5]:- Domain	**Techniques**	**Potency**	**Resilience**	**Cost**
Transform	Code	Medium	One-way	Free
Transform	Data	High	Two-way	Cheap
Transform	Control	Medium	Partial One-way	Costly

There are various forms of technical protection of intellectual property which are available to software developer.

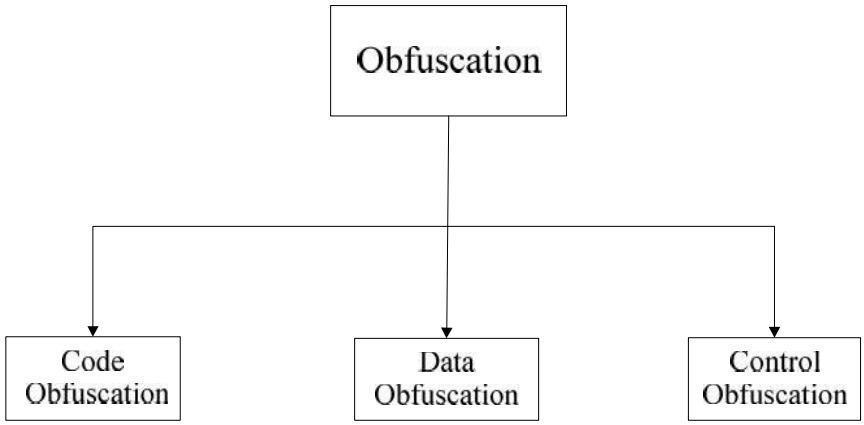

Figure 1.4 Obfuscation Types

Based on above criteria, some of useful techniques of obfuscation are given below.

- ✓ **Character Scrambling**: reordered the characters that are the part of statement which looks like original values are obfuscated.
- ✓ **Repeating Character Masking**: some of first character is replaced by "*" and the last of few just displayed as it is.
- ✓ **Numeric Variance**: numeric value is changed by some other numeric values in some range.
- ✓ **Encoding**: to present the value, some series of character are chosen.

1.4 Cryptography

Cryptography comes from the Greek word "*Kryptos*" meaning "*hidden or secret*" and the "*graphic*" means "*Writing*". In other words, the cryptography is the practice or study of hiding information. Cryptography is considered as a branch of computer science as well as mathematics also. It is used for security of different areas viz. ATM cards, computer password and electronic commerce.

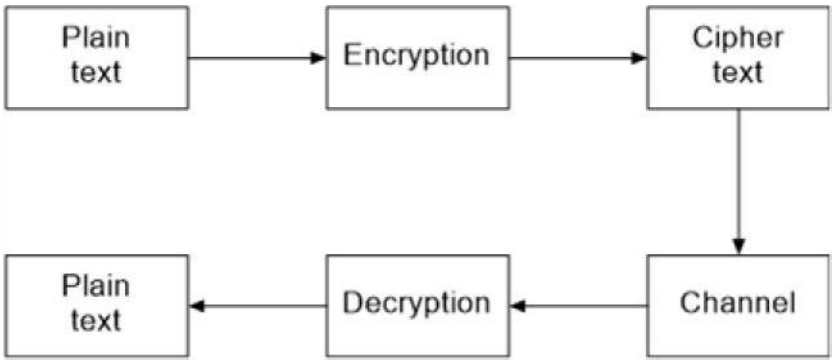

Figure 1.5 General Configuration of cryptography

As shown in the figure the general configuration of cryptography uses Encryption and Decryption methods for converting the plaintext to the cipher text. Cryptography is of mainly 3 types:

1. Secret key cryptography(SKC)
2. Private key cryptography(PKC)
3. Hash Function

These are the types of cryptography which uses the key for encryption and decryption process. In hash function no keys are used but the plaintext once converted into hash code than the plaintext will not be recoverable.

1. **Secret key cryptography(SKC)**

   This uses the single key for both encryption and decryption process. Secret key Cryptography is also termed as symmetric key cryptography as it uses only one key. The key distribution is major factor affecting the Secret key cryptography. The scenario of Secret key Cryptography is shown in below figure**.**

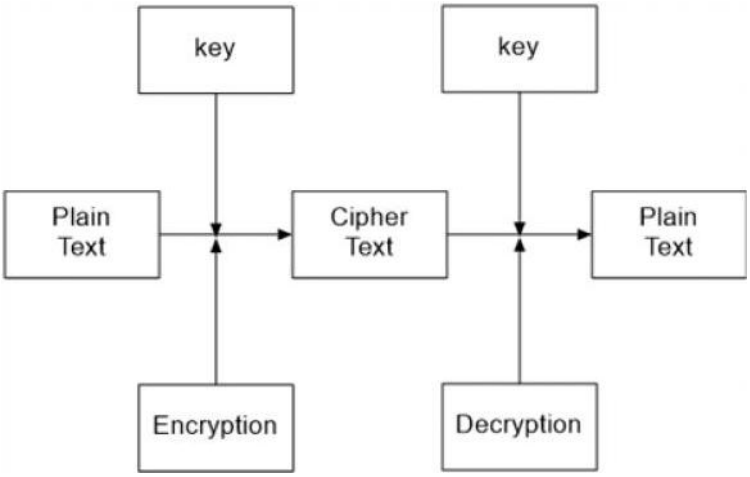

Figure 1.6 General scheme of Cryptography(Secret key)

2. Public key Cryptography

The public key Cryptography uses the pair of key or different keys for both encryption and decryption process. Public key Cryptography is also term as asymmetric key cryptography as it uses different keys. The public key cryptography is often used to secure electronic communication over open network**.** The diagrammatic representation of public key cryptography is shown in below figure.

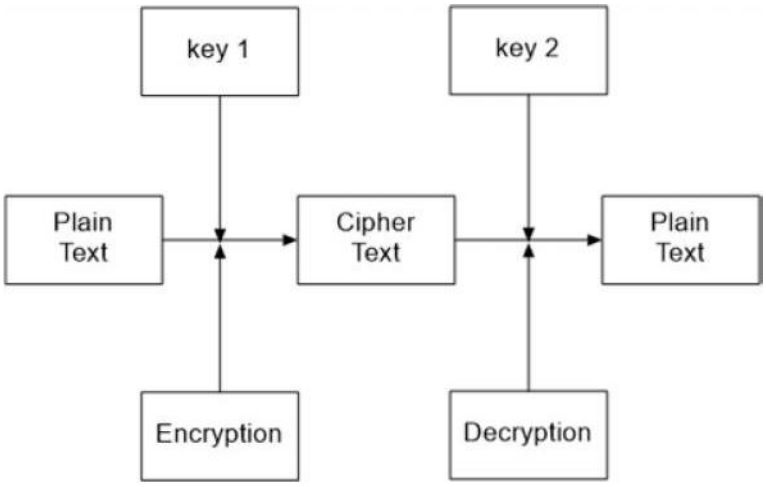

Figure 1.7 General scheme of Cryptography(Public key)

3. Hash Function

The Hash Function is also term as one-way cryptography because the plaintext is not recoverable from the cipher text. The hash function does not use any keys for encryption or decryption, this function is fulfilled the integrity requirement of

cryptography. It provide the integrity of the data in communication. The major factor affecting the hash function is the plaintext is not converted to its original form, below shows the general configuration of hash function.

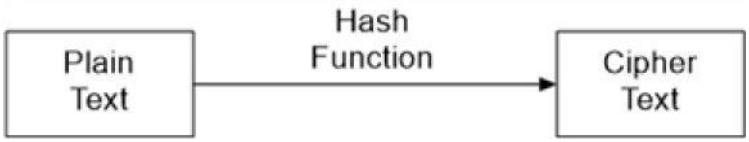

Figure 1.8 General scheme of Hash Function

Requirement of Cryptography

Following are the requirements of cryptographic technique:

1. Confidentiality

   Restrictions on the accessibility and distribution of information OR Protecting the data from unauthorized access or viewing.

2. Integrity

   Protecting data from modification or deletion by unauthorized parties OR What data sender sends; receiver should get the same data.

3. Availability

   Ensures that information or resources are available when required. This guarantees when needed services are always available .

4. Key Management

   This allows negotiating, maintaining and setup keys between communicating entities.

5. Non Repudiation

   Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication

Thesis Organization

Chapter 1: This chapter starts by introducing various basic technology. First describe the Basics of Cloud computing including the Cloud services, Models, Life cycle Etc. Then in next part, detailed description about the Obfuscation mechanism is given which includes

details about obfuscation mechanism, how it works and available types of obfuscation. Lastly, the Cryptography techniques with types and the functionality are described.

Chapter 2: In this chapter, the requirement of the Security in Cloud computing is described. Various levels of security are mentioned and also focus on how the obfuscation helps to improve the security in Cloud environment.

Chapter 3: In this chapter, the gap found is defined and the aims and objectives that we need to satisfy with our proposed model.

Chapter 4: In this chapter , the views given by various researcher are presented related to the thesis work. We also compare the existing proposed work by using various parameters that are offered by the proposed scheme of various researchers.

Chapter 5: This chapter contains the detailed description of proposed scheme where the model followed by the description of all phases is illustrated.

Chapter 6: In this chapter, we provide the implementation details where the screenshot of various phases of the model is provided.

Chapter 7: It consists the discussion pertaining to findings and result found which is followed by graphs and chart notation. We also describe the security of proposed methodology by applying security tool. Finally, technical comparison of the model using various parameters with known phenomenon are devised.

Chapter 8: At the end I conclude overall process by giving conclusion and also mentioned some future direction that can be possible if wants to extend the model Followed by reference and remaining sections.