Secure Cloud Using Cryptography

Saharsh, Shubham Srivastava*, Lavanya M C

Dept. of Information Science & Engineering, The National Institute of Engineering

DOI: https://doi.org/10.21467/proceedings.1.49

* Corresponding author email: shubham1995srivastava@gmail.com

Abstract

Cloud Computing is one of the mot liked and diverse topic in today's world. It is a blend of number of different technologies. Decrease in cost, load, is one of the major advantages of this new technology. There has been an exponential growth in the usage of data, thereby, increasing need of data confidentiality. By confidentiality of data we mean protecting of data from unauthorized entities. Encryption is one of the most used methods for the security of data. It is very easy to use, and also different cryptographic algorithms are available to be used for encryption. Cloud Storage provides scalability, cost efficiency, and access of data anytime and anywhere. These all factors lure different organizations to use this cloud storage and use it as their primary storage service provider. It also overcomes the problem of denial of services. In this paper, the plan proposed is to overcome the issues regarding the data privacy using cryptographic algorithms and to elevate the security in cloud as per different organizations. Cloud computing provides a foresight in elasticity, flexibility and on demand storage and computing services for users. In his type of concept, data owner does not have full access over their own data and is controlled by cloud service provider. Our motive is to provide data confidentiality, access control of shared data, removing the burden of key management of users, owner does not have to be always online to access when the user wants to access the data. This paper's main aim is on cloud storage services and its security, i.e., using cryptographic algorithms for securing data and its computation on cloud platform.

Index Terms- Cloud computing, Elliptic Curve Cryptosystem ,Confidentiality Integrity Authenticity, Cloud Service Provider

1 INTRODUCTION

In cloud computing, enormous amount of data is scattered across different storage servers. There are many techniques to store data on server. The basic principles of any storage devices is to provide CIA. Confidentiality refers to restricting the access of data. It is important to maintain an owner's data privacy which he/she is putting somewhere else. By integrity we mean data should be protected against accidental or intentional alteration without having authority. Availability means being able to use the system as per user requirement. Cloud computing composes of both hardware and software resources and is managed by third party

services. These services provide authority to access software application and high end networks of computer servers. Cloud computing confers remote services with users data, software and applications. Cloud computing uses networks of number of group of severs running low cost consumer PC technology to spread data processing job across them. The IT infrastructure contains large pools of systems which are linked together.

It is important to supervise our data and to preserve its sensitivity. For this we need a secure storage which is provided by cloud computing. So we can use cryptographic techniques, the data is encrypted by the data owner before it is uploaded to the cloud. Therefore, whenever the data will be downloaded by the user, it will always be in encrypted format. The encryption algorithm is a technique to protect data within cloud environment. Client's data can be either public data or private data. Public data is sharable amongst trusted clients and private data is client's confidential data that must be in encrypted form for security and privacy. Cryptosystems can be classified into symmetric and asymmetric.

In symmetric cryptography, the receiver and sender share a decryption key and an encryption key. These two keys are the same or easy to deduce each other. We have an AES encryption algorithm which is faster and superior under the scenario of data transfer. The popular asymmetric encryption algorithms are RSA and elliptic curve cryptography. These algorithms are compared on the basis of key size, features such as, key generation time, signature generation and verification time. With RSA, signature generation and verification time is much less than ECC. But ECC scores over RSA because of less key generation time. That's why we prefer ECC over RSA. To have data authentication and non-repudiation technologies like digital signature has acquired great significance. For example, MD5 and SHA-1 are well known digital signature generation algorithm.

2 LITERATURE SURVEY

Many works have been done in the field of cloud security in recent times. Akansha Deshmukh et al. [1] proposed that data generated by the organizations is growing exponentially, data is stored in cloud by CSP's. The main aim is to provide data authentication, integrity and confidentiality using cryptographic algorithms. Punam V.Maitri et al. [2] showed that cloud computing is useful in many fields for data storage purposes, there are n number of ways to provide data security, here symmetric key cryptography and steganography algorithms are used. Dr.G.Jaspher et al. [3] proposed that cloud is a omnipresent computing technology, day by day cloud computing is enhancing so its security is important such as access control, storage, virtualization. Biometric based authentication is proposed. We try to implement a model using Microsoft Azure for using cloud services. The encryption and decryption algorithms, i.e., DES and RSA, were embedded in the code. We have used PHP for web page development and for encryption and decryption. To provide protection for business data we have BitGlass, which is a beta version and provides transparent protection. It aims to reduce the risk of data loss and maintains data visibility.

ISBN: 978-81-936820-0-5

Series: AIJR Proceedings
Proceedings DOI: 10.21467/proceedings.1

3 SYSTEM DESIGN

Cloud service provides the user with shared infrastructure, adopting firewalls, management consoles, load balancers, and APIs. The cloud services are disrupted by virus attacks, even some misconfiguration issues, as well as inadequate user policy settings which could lead to errors. To avail the feature of continuous availability and best services cloud security architecture should be designed to withstand various disruption. It should also be in accordance with the technology architecture as well as the organizational principles. One needs to establish standard framework such as ISO-27001, CSA and CCM are major aspects to be followed. Also, the CCMC should run in parallel to organizational security policies and practices. Cloud security architecture plays a vital role in the safety of files. Having a right security system could control and protect the information which could mitigate the threats in cloud security. Security control could be embraced by the cloud service enterprise from a third party provider, or as a service during export and import of security event logs, user privileges, change management logs, user profiles, or enterprise log standard format. Overall, continuous security monitoring such as cloud audit have become an integral part of cloud security. Figure 1 shows secure data sharing in cloud computing.

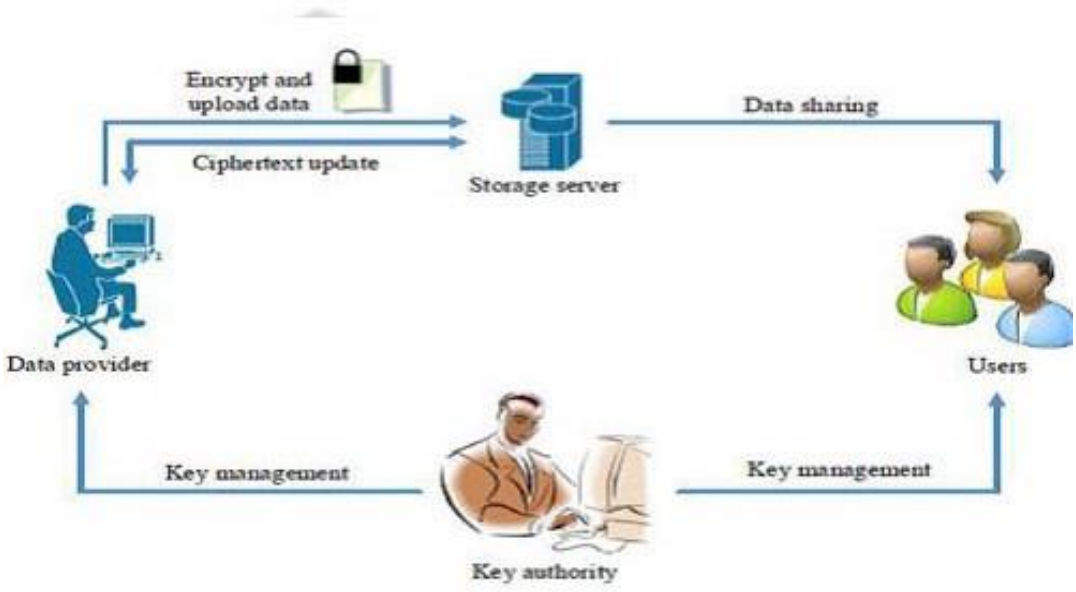

Figure 1: Secure Data Sharing in Cloud Computing

Personal Cloud Storage security challenges can be overcome by combining two different security algorithms. A combination of DES and RSA algorithm has been chosen here. In DES, a single key is used for both encryption and decryption of data whereas in RSA two different keys are used for encryption and decryption. When a user uploads a text file in personal cloud storage, DES and RSA encoding schemes are used to encrypt the data. A file

is being encrypted not by just using one but three encryption algorithms, i.e., AES, DES, and RC6 which makes the stored file completely secure. The key is embedded in an image using LSB which makes the key also safe. Unauthorized access on cloud server is prohibited which keeps the data secure. The RSA algorithm was developed by Ron Rivest, Adi Shamir and Leonard Adleman. RSA is a type of public key cryptography system which uses both, a public key and a private key. For encryption, public key is used. For decryption, private key is used. Figure 2 shows this algorithm.

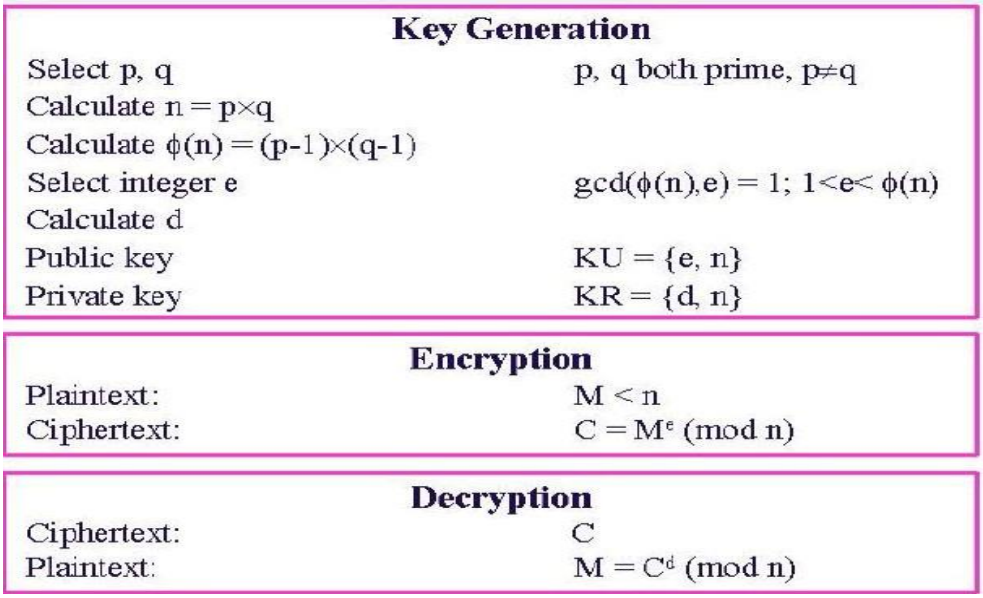

Figure 2: RSA Algorithm

In the above figure, e is the public key, d is the private key, M is the plaintext and C is the ciphertext.

At the encryption side, $C = M^e \bmod n$.

At decryption side, $M = C^d \bmod n$. Here, n is a very large number created during key generation.

A DFD is used to represent system components and the flow of data. It can also be used to represent a system in terms of input, process and output. It shows the flow of information in the system and how it is updated by a series of modifications. A system can be represented at any level of abstraction by the help of a DFD. DFD is divided into many levels that depict information flow and functional detail. DFD scans the current physical system, generates input output specification and tells the implementation plan. Four basic symbols are used to represent data source, data flow, data transformation and data storage in a flow diagram. Nodes are used to represent the stages where data is transformed and are usually represented by circles. A system's high level detail can be modelled using DFD as it shows the transformation of input data to output information by a series of functional modifications. The four major components of DFD are entities, processes, data storage and data flow. Simple

ISBN: 978-81-936820-0-5
Proceedings DOI: 10.21467/proceedings.1

and easy to understand symbols are used to represent how these components interact in a system. Figures 3, 4 and 5 show the DFD of various system instances.

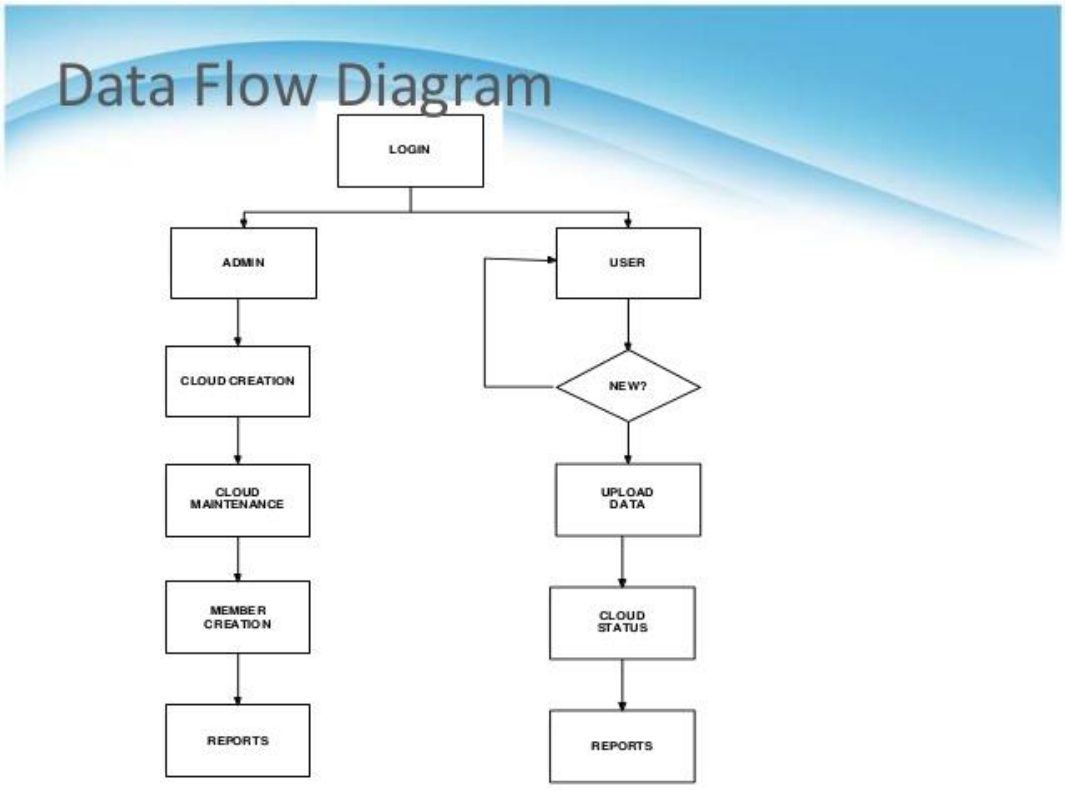

Figure 3: Data Flow Diagram for User

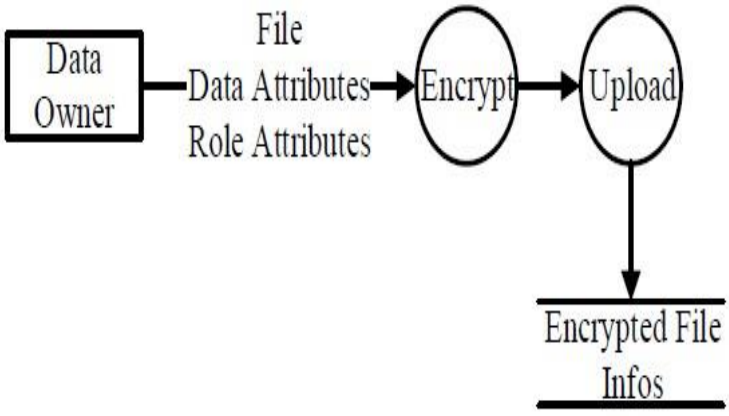

Figure 4: Data Flow Diagram for Encryption and Upload

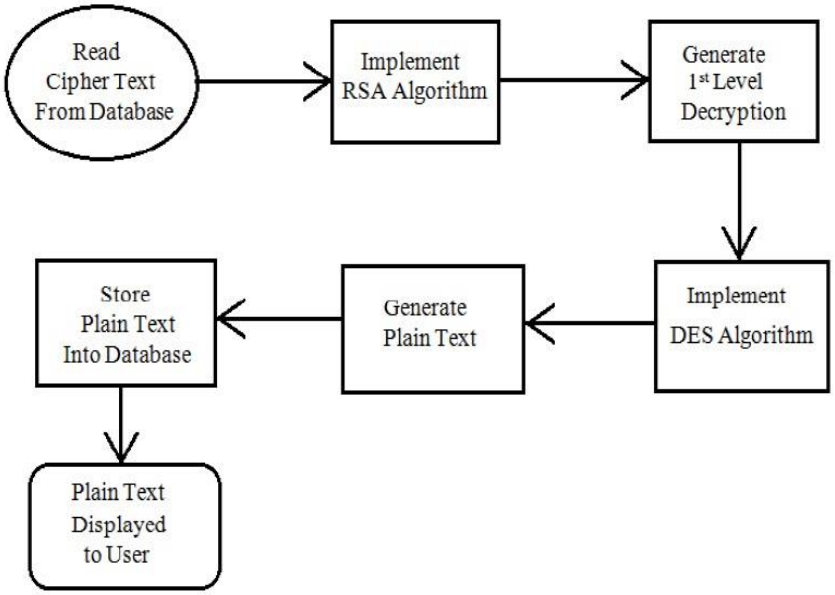

Figure 5: Data Flow Diagram of Multilevel Decryption

An activity diagram is a graphical representation of step-by-step workflow of components in a system. Figure 6 shows the overall control flow of the system.

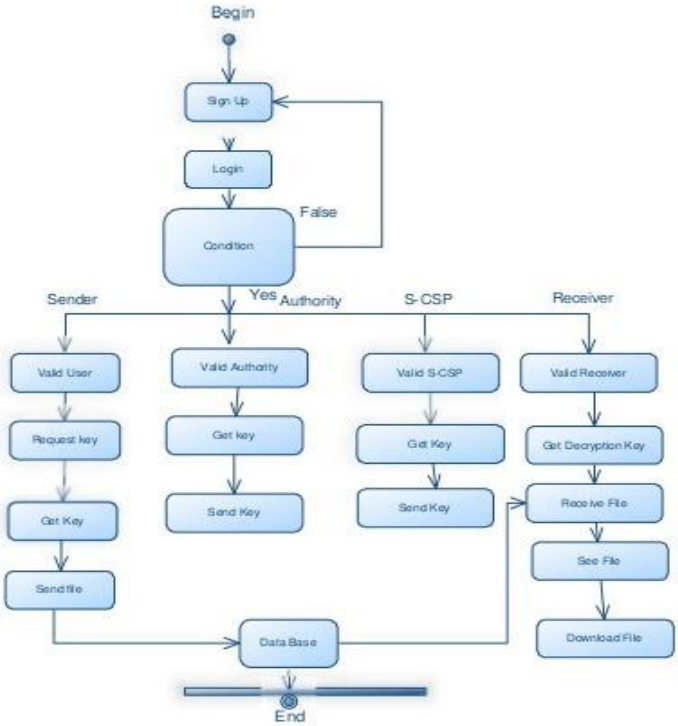

Figure 6: Activity Diagram of the system

The implementation phase consists of four different modules namely, client module, storage of data module, cloud authentication process, secure data modification. In the client module,

ISBN: 978-81-936820-0-5
Proceedings DOI: 10.21467/proceedings.1

Series: AIJR Proceedings

a request to the server is sent by the client in the form of a query. Before sending request to the server, a client should authenticate himself/herself. In the authentication process, the client's username and password is verified for security purpose. If the details are correct, the user is authenticated and the request is processed. The request file is searched by the server and if found then it is provided to the user. If the server finds an intruder, then an alternate path I set for the intruder.

The storage of data module deals with the storage part. In cloud computing, the user data is stored on cloud servers which run different systems simultaneously. The data is stored on different data servers which are maintained by the cloud service providers. The stored data should be secured. There are many users logged in to the system which makes it difficult to monitor the performance of the system. Third party auditors are used to maintain the security and feasibility of the system. The cloud authentication process is the first process which is run. It authenticates a user by checking the provided username and password. There are some additional behaviors associated with the authentication server. At first, the client authentication information is sent to the masquerading router. Whenever any user want to access any file, a token is generated which is issued by the ticketing authority and controlling permissions are applied to enforce security. The authentication server also updates the client list which reduces the authentication time. It is also responsible for removal of clients. The secure data modification module deals with the changes to the secure data. If any user wants to insert or delete his data or files, this means the user will be operating at block level, so authentication becomes important here.

4 CONCLUSIONS

Cloud computing is defined as a collection of resources and service deployed over internet on the demand requested by users. Since in this new data age, every organization is generating a huge amount of data and are thus using the storage services provided by cloud service providers, since the information critical data is stored on the cloud there is a need to provide security against unauthorized modification, unauthorized access and denial of services.

References

[1] Akansha Deshmukh; Harneet Kaur Janda; Sayalee Bhusari; "*Security on Cloud Using Cryptography*".2015 In International Journal of Advanced Research in Computer Science and Software Engineering.

[2] Punam V.Maitri; Aruna Verma; "Secure File Storage in Cloud Computing Using Hybrid Cryptography Algorithm". 2016 IEEE WiSPNET 2016 conference..

[3] Dr.G.Jaspher; Willsie Katherine; "*A secure framework for enhancing user authentication in cloud environment using Biometrics"* 2017 International Conference on Signal Processing and Communication(ICSPC'17).