International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 04 | Apr 2019 www.irjet.net p-ISSN: 2395-0072

Secure Data Protection in Cloud Computing

Rahul Midha[1], Simran Khajuria[2], Suman Samal[3], Aishwarya Mishra[4]

[1,2,3,4]*Computer Science Engineering Student, Bharati Vidyapeeth's College of Engineering, New Delhi*

Abstract - *Cloud computing is way to store data in a "virtual" cloud. Virtual means something that is not present physically but still exists. The cloud computing allows a user to store their data. The amount of data stored in cloud is adequate. But there is an issue which limits the use of cloud computing is security, so cloud computing precipitate security solutions. The simplicity and ease of use made everyone use cloud for data storage. The cloud service provider (CSP) is responsible for reliability, security, privacy and availability of data. But the CSP doesn't provide the user full security, as once the data is uploaded in cloud, the CSP have full control over the data but the user doesn't. The CSP could perform any activity with the user's data. This lack of control over the data leads to greater security issues. This paper presents secure storage of data and securing it from unauthorized access by giving access to garbage files. To detect the authenticity of the person, Honeypot Technology is used. This technology detects and counter attacks the unauthorized access by generating a garbage file. Data security is improved by using cryptographic algorithm.*

Key Words: **Honey Pot, Cloud service, encryption, decryption, security, Cloud computing**

1. INTRODUCTION

Cloud Computing has been considered as a next generation model in computation. In cloud computing, both applications and resources are provided on seeing demand over the internet services. Cloud computing is an area of the hardware and software resources in the centers of data where that provide service over the network which are secure [1]. The meaning of "Cloud Computing is quite well explained by the National Institute Of Standards And Technology (NSIT) [2] which is cloud computing makes one ubiquitous, convenient, on demand network access to a shared number of configurable computing resources that can be supervised and released with less management effort .The three very well-known and mostly used service models in a cloud platform are " Software As A Service"(SaaS), "Platform as a Service" (PaaS) and" Infrastructure as a Service"(IaaS) .In SaaS , software with the related data is controlled by cloud service provider and users can access it through the Web Browser. In PaaS, a service provider provides services to you and users with some set of software programs that can resolve the problem statement. In IaaS, the cloud service provider provides the user with virtual machine and storage to improve their strategies. We can say cloud computing is mostly related to but not exactly same as grid computing [3]. The whole scenario of grid computing has been changed when cloud computing was introduced. Cloud computing is a blessing for IT application, however there are still some shortcomings which needs to be solved for personal users and enterprisers to store data and deploy application in the cloud computing environment. One of the most important barrier is to adopt data security which is accompanied by issues such as privacy, trust and legal matters [4]. Data Security is one of the most important ingredients of a system in order to ensure QoS (quality of service). Most importantly cryptography technique used for the purpose of data security protection cannot be directly adopted due to the users' loss control of data under Cloud Computing. Therefore, verification of correct data storage in the cloud must be conducted without explicit knowledge of the whole data.

From the view of data security, which has always been an important aspect of quality of service, Cloud Computing inevitably poses new challenging security threats for number of reasons.

1.1 EXISTING SYSTEM

The existing systems focus and target at providing integrity and storing the data but the problem of confidentiality still exists and still isn't resolved completely. All these systems doesn't ensure the security and are unable to provide security assurance to users.

Disadvantages of existing systems:

Existing systems are unable to provide complete security assurance to users.

1.2 PROPOSED SYSTEM

The proposed system aims to provide better security aspect to the user. The proposed system uses the concept of Honeypot technology along with cryptographic tools to provide better security to the saved data. Once the data is saved over cloud, it could only be accessible by the user using their personal credentials, if any unintended person tries to access the data using false credentials it will send a garbage file using honeypot technology.

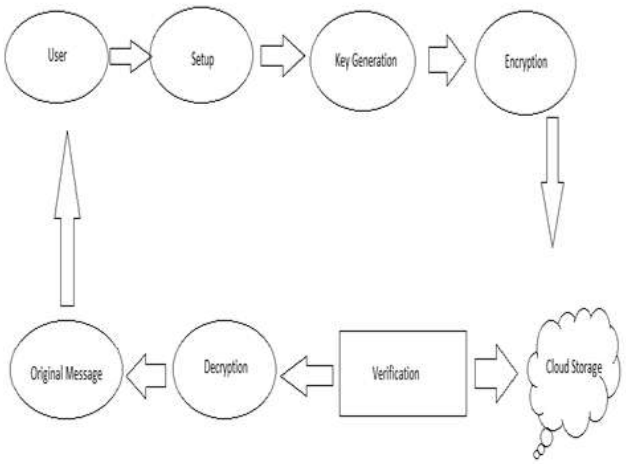

Fig. 1 – Implementation Framework

2. LITERATURE SURVEY

The basic aim behind private key cryptography is to provide end to end authentication to the data of the user. The data is stored in the form of a hierarchy with the help of secret keys which have a non-constant size. In order to obtain a child key from a parent key, hash functions are used for this purpose. All the confidential information is stored in the hierarchy locally on the system, with space complexity being optimal in nature. All the file updates are stored and handled on the system locally. The encryption scheme used can be used for transmitting any number of keys [5]. This encryption scheme provides partial access rights to the user, along with the functionality of traversing the records stored in the system. Different cryptographic primitives stores protocols and settings with unique properties. In order to encrypt a particular file, the associated secret keys are used, which may or may not be suitable for many applications. The public key of the data is used as the identity string for uniquely identifying a user over a system. A private key generator is used to build a master key, which then issues a secret key to the intended user for data access. The data can be decrypted by the user by making use of this secret key. This method is known as Identity Based Encryption [6].

Another method that can be used is Attribute Based Encryption [7]. In this method, each attribute of a file is associated with a cipher text. The master key is used to extract the secret key for these attributes in order to provide access to them, if it adheres to the prescribed policies.

But, the drawback with attribute based encryption is that the secret keys consume a lot of space, as it has multiple attributes associated with it, thus leading to a large access time, slowing down the overall performance of the system.

3. RESEARCH METHODOLOGY

Our aim is to provide a secure cloud access to all the users of a system, where they can store their files in encrypted form. For this, an encryption/decryption scheme is required in order to perform this operation. After exploring all the available approaches, RSA algorithm proved to be a feasible option for this project. It's an asymmetric cryptographic algorithm. This implies that it has 2 different keys, one being the public key, and the other is a private one. The role of public key is to encrypt the files stored on the cloud, and its access is provided to everyone. The files encrypted by public key, and stored on the cloud, can only be decrypted by making use of private key.

Also, in order to ensure security of data, the concept of honey pot is also implemented on this project. Honey pot is a concept that's used to handle unauthorized access to files in a system, by detecting and counteracting the attempts of a system breach. In honey pot, the unauthorized users are presented with an illusion of data present at a location, which isn't the actual data of the user. The actual data is stored in encrypted form, in an isolated file system, which can only be accessed by authorized users of the data. Honeypot can be classified into 2 categories broadly –

1) Production Honeypot
2) Research Honeypot

Production honeypot is used at a small scale, which can gather a very limited amount of information. It's used by small enterprise firms, and is easy to deploy privately in the production network. The amount of information given by production honeypot is inadequate, and doesn't contain all the necessary details of the attack.

Research honeypot is a large scale version of production honeypot, and is used to gather information about the hackers that are planning to exploit a network by intruding in it. Research honeypot is also used to learn about what are the possible threats to a system, by different hackers, and how can it be avoided by safeguarding the system against those attacks. Research honeypot is difficult to deploy, due to its complex nature, as it's designed to capture a large amount of information. Also, the modelling approach used in this project is "RUP (Rational Unified Process)" modelling. RUP provides a full lifecycle approach covering a series of product lifecycle phases called inception, elaboration, construction, and transition.

It's incremental in nature; each iteration builds on the functionality of the prior iteration; the software application evolves in this fashion with the benefit of regular and continues feedback. RUP consists of four phases which can be altered to suit the needs. As iteration is a key feature of the model, it's very useful for the development of a project as developer requires a repetitive check of the key features.

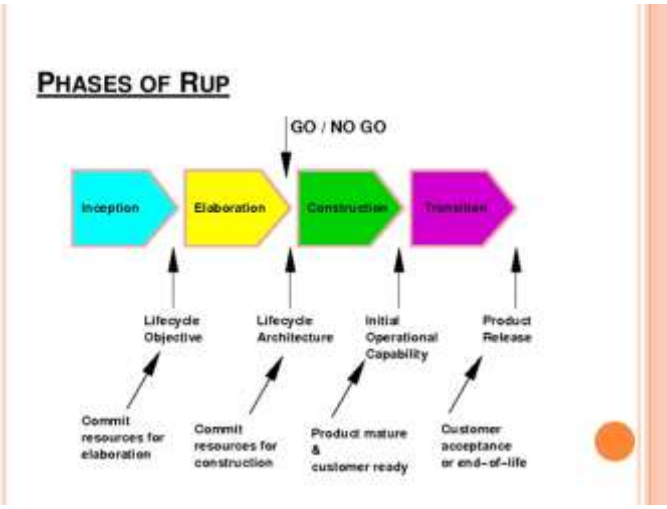

Fig. 2 – RUP Modelling

4. IMPLEMENTATION

In this model, a local machine server or local host is used to depict the working of a cloud. It provides user with the resources to store data and act in accordance with the hardware and software specifications of the cloud. Our machine acts as a server. We stored files and application on the server and it fulfilled the entire user's requirements like fast and remote processing, proper resource allocation etc. and is therefore appropriate for demonstration.

We in this paper propose various methods for data security in cloud. Since security in a cloud environment is at stake and the traditional cryptographic methods don't work, therefore we had to implement an efficient cryptosystem to deal with this issue. We tried encrypting with block cipher methods, stream cipher methods, and erasure code but finally used a type of public-key cryptosystem called RSA which is a simple but robust encryption technique [8]. The user stored his file on our machine. The file was encrypted using a public key and stored on the local host, such that a private key was generated and given to the user for decryption. This implies that the message could be encrypted by anyone but decrypted only by the authentic user (this gives it a first degree of security).

To further improve the security we have used the concept on honeypot here. Honeypot is a technique used in computer security to detect and deter malicious attempts at data breaching and unauthorized access of data. The main files and applications were emulated and kept at a separate location and resembled the original programs or applications [9]. The honeypot had all the relevant information needed by the hacker and as the hacker would try to access the honeypot, his activities would be recorded and he would be presented with cipher text which would make no sense to him. Thus, we isolated the original file from the cipher file of honeypot.

Another important aspect we present in this paper is dynamically updating the data in the cloud model while maintain data integrity and security [10]. While updating information: append, delete or modify the data is vulnerable as the user interacts with the server and some intermediate host could perform the act of sniffing and breach the security. We in this model have used homomorphic tokenization to operate on the sensitive data such that we are able to operate on the encrypted data itself [11]. Finally bypassing all the malicious acts the integrity of file was maintained and the user was finally able to decrypt and access his file using the private key that was allotted to him.

5. RESULT

The proposed system encrypts the data using RSA and uploads it to the cloud securely. The system verifies the keys if the keys matches, it decrypts the data and provides access to the user whenever prompted. If the entered key doesn't matches it sends a garbage file using honeypot technology.

6. CONCLUSION AND FUTURE SCOPE

When a user stores its data in cloud, its always a matter of concern if the CSP is providing proper security and privacy to the user, and if the data is not mishandled and misused. Security and privacy are always the main concern of cloud computing. In the proposed system a secure mechanism is provided to store data securely over cloud. This system provides integrity, authenticity and confidentiality to the data stored in cloud. Authentication is achieved by giving access of the stored data only to registered client. Only registered client could upload and download files on the cloud. The system is intended to secure data using the combination of RSA and honeypot technology. This ensures that no leakage of data is possible. The data is always encrypted first and then uploaded, the keys are matched and then only it gives the access.

Further, this model could be improvised with better upcoming technologies to ensure the data security.

REFERENCES

[1] N. Lavitt , "Is the cloud computing really ready for prime time?" computer vol. 42, no. 1, pp. 15 -25, 2009.

[2] P.Mell and T.Grance "the nist definition of cloud computing", National Institute Of Standards And Technology, vol.53, no. 6, article 50 , 2009.

[3] F.B er man , G.Fox and A.J.G. Hey, Grid Computing : Making the Global Infrastructure a Reality, Volume 2, Jhon Wiley and Sons , 2003.

[4] M.A. Shah , R. Swaminath and M. Baker, "Privacy preserving audit and extraction of digital content," IACR Cryptology EPrint archive, volume 186, 2008

[5] M. J. Atallah et.al, "Dynamic and Efficient Key Management for Access Hierarchies," ACM Transactions on Information and System Security (TISSEC), vol. 12, no. 3, 2015.

[6] J. Benaloh et.al, "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records," in Proceedings of ACM Workshop on Cloud Computing Security (CCSW '09). ACM, 2014, pp. 103–114.

[7] M. Chase and S. S. M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," in ACM Conference on Computer and Communications Security, 2017, pp. 121–130.

[8] Smart, Nigel (February 19, 2008). "Dr Clifford Cocks CB". Bristol University. Retrieved August 14, 2011.

[9] Cole, Eric; Northcutt, Stephen. "Honeypots: A Security Manager's Guide to Honeypots"

[10] B. Anjani Kumar, K. Hari Prasad, C. Subhash Chandra , "Homomorphic Token and Distributed Erasure-Code for cloud", International Journal of Research in Computer and Communication Technology, Vol 2, Issue 10, October-2013

[11] Gentry, Craig. "Fully Homomorphic Encryption using Ideal Lattices". *ACM Symposium on Theory of Computing, STOC 2009*. pp. 169–178.