Effective Key Management for Data Security on Cloud

V. Vijayakumari[1] S. Kousalya[2] S. Poongodi[3] M. Saravanan[4]
[1]Assistant Professor [2,3,4]BE Student
[1,2,3,4]Department of Computer Science & Engineering
[1,2,3,4]The Kavery Engineering College, India

Abstract— computing is an on-demand access to a shared pool of configurable computing Cloud resources. Cloud services are delivered from data centers located throughout the world via internet. security for cloud computing in many threads in store to access the third party attack the data in cloud. To provide security for the data have to use encryption and decryption technologies. In this Paper to generate the key by using RSA algorithm and data can be encryption & decryption by using AES algorithm. AES data encryption is more scientifically capable and graceful cryptographic algorithm, AES allows you to choose a various type of bits like 128-bit, 192-bit or 256-bit key.

Key words: AES, Could Computing, DES and RSA

I. INTRODUCTION

The Cloud Computing becoming a popular term on the IT market security and accountability has become important issues to highlight. There are a number of security issues/ concerns associated with cloud computing but these issues are fall into two broad categories: Security issues faced by cloud providers (organizations providing Software, Platform, or Infrastructure-as-a-Service via the cloud computing) and security issues faced by their customers. In most cases, the provider must ensure that infrastructure is secure and that their clients' applications and data are protected while the customer must ensure that provider has taken the proper security measures to protect their information. Cloud computing has emerged as a way for IT businesses to increase capabilities on the fly without investing much in new infrastructure. It follows a simple "pay as you go" model, which allows an organization to pay for only the service they use. It eliminates the need to maintain in-house data center by migrating the enterprise data to a remote location at the Cloud provider's site. Minimal investment, cost reduction, and rapid deployment are the main factors of the drive industries to utilize Cloud services and allow them focus on core business concerns and priorities rather than dealing with technical issues. Cloud services are offered terms of IaaS, PaaS), and SaaS. It follows a bottom-up approach wherein at the infrastructure level; machine power is delivered in terms of CPU consumption to memory allocation. It lies on the layer that delivers an environment in terms of framework for application development, termed as PaaS. At the top level of resides the application layer, delivering software outsourced through the Internet, eliminating the need for the house maintenance of sophisticated software. At the application layer, end users can utilize the software running at a remote site by Application Service Providers (ASPs). Here, customers need not buy and install costly software. They can pay only for the usage and their concerns for maintenance are removed.

II. EXISTING SYSTEM

This Existing system explains that

A. Client Authentication

This module includes testing the clients for his nor her credibility by closing username and secret key confirmations. There may be 2 sort of buyers take a shot at to the server:

- New Users
- Existing Users

New Users might give a required username and password which can be superimposed to the illumination on the server. Existing clients might confirm their personality by giving their remarkable username and password. This module handles key by the server viewpoint. The server produces unique keys for clients once they show themselves with the server. The privileged insights created abuse occurrences of class. AES key generator The mystery's a sixteen workstation memory unit or a 128 bit key Fully Homomorphic Encryption Notwithstanding the Keygen, Encrypt, change methodologies of PKE (Public Key coding) plans, these plans give a further govern survey.

B. Disadvantages for Existing System

- Outsourcing data to the cloud is economically attractive for long term large scale storage it does not immediately offer any guarantee on data integrity and availability.
- Data security protection cannot be directly adopted.
- It does not give users correctness assurance for those unaccessed data and might be too late to recover the data loss or damage.

III. PROPOSED SYSTEM

- The main focus of our project to improve a data security using AES and RSA algorithm based on cloud.
- A third party auditor is introduced for the protection of shared data for cloud sever
- The audit result from TPA would also be beneficial for the cloud service provider to improve their Cloud based service platform.

A. Advantages of Proposed System

- A public verifier is able to correctly verify the shared data integrity.
- A public verifier does not distinguish the identity of the signer on each block in shared data during the process of auditing.
- To support scalable and efficient privacy preserving public storage auditing in cloud

IV. IMPLEMENTATION

A. Module Description

- Cloud setup.
- User interface design.
- Key management or key generation.
- Encryption And Decryption using AES Algorithm.

All rights reserved by *www.ijsrd.com*

B. Cloud Setup

- Cloud setup module is using the cloud sim tool.
- Cloud sim is a framework for modelling and simulation of cloud computing infrastructure service.
- Cloud sim support for modelling and simulation of large scale cloud computing data centers.

C. User Interface

Fig. 1: Screenshot

V. KEY MANAGEMENT

A. RSA Algorithm

RSA algorithm is one of the first practical public key encryption cryptosystems and widely used for secure data transmission. In such cryptosystem, the encryption key is public and differs from decryption key which is secret. In RSA, this asymmetry is based on the practical difficulty of factoring product of two large prime numbers. RSA is made of the initial letters of the names of Ron Rivest, Adi Shamir, and Leonard Adleman, first publicly described the algorithm in 1977. Clifford Cocks, an English mathematician has developed an equivalent system in 1973, but it was not declassified until in 1997. A user of RSA creates and publishes a public key based on two large prime numbers, along with an auxiliary value. The prime numbers must be secret, anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime numbers can feasibly to decode with the message in breaking RSA encryption is known as the RSA problem whether it is hard as the factoring problem remains open question data is split into number of parts and each part will be stored at different server. The data will be stored in database initially, the user upload a file. A hash key is generated at the user and also at database. The database check whether is already exist a copy of user data, if it is exist then only hash key will be generated but the data will not be uploaded to avoid the de-duplication(data duplication).Then the TPA checks the data authentication also provide security to data. As the data is uploaded on the server load balancing take place at each server.

B. AES Algorithm

The more popular and widely adopted symmetric key encryption algorithm likely to encountered nowadays by Advanced Encryption Standard (AES). It is found at faster than triple DES.

A replacement for DES was needed as its key size was too small. It was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow.

The features of AES are as follows −

- It uses 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java

VI. WHY SECURITY IS IMPORTANT IN CLOUD:

Security and privacy at the forefront of buyers' and providers' minds in relation to cloud services. Security (88%) and Privacy (73.3%) topped the list of buyers' primary hesitations in deciding whether to buy cloud services.

The importance of security was evident in identifying buyers primary criteria for choosing a provider. A majority of buyers identified published security terms and compliance as such criteria.

VII. IMPORTANCE OF KEY MANAGEMENT

Key management is the management of cryptographic keys in cryptosystem. This includes dealing with generation, exchange, storage, use, and replacement of keys.

Key management concerns at the user level, either between users or systems. This is in contrast to key scheduling.

Successful key management is critical to the security of a cryptosystem.

In practice the most difficult aspect of cryptography because it involves system policy, user training, organizational and departmental interactions, and coordination between all of these elements.

VIII. CONCLUSION

A protected cloud computing environment relies on upon a few security results working concordantly together. Be that as it may, in our studies we didn't recognize any security results supplier owning the offices important to get large amounts of security similarity for clouds. In this Paper To generate the key by using RSA algorithm and data can be encryption & decryption by using AES algorithm. AES data

All rights reserved by *www.ijsrd.com*

encryption is more scientifically capable and graceful cryptographic algorithm, AES allows you to choose a various type of bits like 128-bit, 192-bit or 256-bit key.

REFERENCES

[1] Vanya Diwan, Shubhra Malhotra, Rachna Jain, Cloud Security Solutions: comparison among various Cryptographic Algorithms, International Journal of Advanced Research in Computer Science and Software Engineering, New Delhi, India.
[2] RashmiNigoti, ManojJhuria, Dr.Shailendra Singh, A Survey of Cryptographic Algorithms for Cloud Computing, International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS), Madhya Pradesh,2010.
[3] K.S.Suresh, Prof K.V.Prasad, Security Issues and Security Algorithms in Cloud Computing, International Journal of Advanced Research in Computer Science and Software Engineering, Hyderabad, 10, October 2012 .
[4] Dr. L. Arockiam, S. Monikandan, Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm, International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 8, August 2013.
[5] Cong Wang, Qian Wang, and KuiRen, Wenjing Lou, Ensuring Data Storage Security in Cloud Computing.
[6] Dai Yuefa, Wu Bo, GuYaqiang, Zhang Quan, Tang Chaojing, Proceedings of the 2009 International Workshop on Information Security and Application (IWISA 2009) Qingdao, China, November 21-22, 2009.

All rights reserved by *www.ijsrd.com*