ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

Security of Cloud Computing using Encryption and Decryption Methods as a Third Party Auditor

Poonam M. Umbarkar [1] Prof. N. R. Borkar[2]

M E. Scholar, Department of Computer Science and Engineering, KGIET, Darapur, India [1]

Professor, Department of Computer Science and Engineering, KGIET, Darapur, India [2]

ABSTRACT: Cloud computing has great potential of providing robust computational power to the society at reduced cost. With the advent of the World Wide Web and the emergence of e-commerce applications and social networks, organizations across the world generate a large amount of data daily. This data would be more useful to cooperating organizations if they were able to share their data. Two major obstacles to this process of data sharing are providing a common storage space and secure access to the shared data. In the New security survey of cloud computing is peoples are very possessive about to store data on cloud because before 2 year some of cloud data is leaked by cloud server. To build the trust for the growth of cloud computing the cloud providers must protect the user data from unauthorized access. So for this issue we will think to secure user data by using Security cloud as a TPA. He will just to encrypt and decrypt user data and send to cloud means if suppose cloud will leak data so he will get data in the encrypted form. Another techniques could be security services like computing hash service if provide for same cloud storage provider. We provide two cloud one for encryption and decryption namely trusted third party which will provide security services and second one is for only storage in that only we have to store the data. The software is only responsible for Encryption/decryption, computing/verifying Hash of data and does not store any data in trusted third party that is security cloud only, Master key is stored in the database for encryption/decryption.

KEYWORDS: Cloud computing, Encryption/decryption service (TPA), Hash service for Data verification and integrity check.

I. INTRODUCTION

The cloud computing service models are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). In a Software as a Service Model, a pre-made application, along with any required software, operating system, hardware, and network are provided. In PaaS, an operating system, hardware, and network are provided, and the customer installs or develops its own software and applications. The IaaS model provides just the hardware and network; the customer installs or develops its own operating systems, software and applications [11].

Cloud services are popular because they can reduce the cost and complexity of owning and operating computers and networks. Since cloud users do not have to invest in information technology infrastructure, purchase hardware, or buy software Licences, the benefits are low up-front costs, rapid return on investment, rapid deployment, customization, flexible use, and solutions that can make use of new innovations. In addition, cloud providers that have specialized in a particular area (Such as e-mail) can bring advanced services that a single company might not be able to afford or develop. Some other benefits to users include scalability, reliability and efficiency. Scalability means that cloud computing offers unlimited processing and storage capacity.

The Cloud is reliable in that it enables access to applications and documents anywhere in the world via the Internet fig 1. Cloud computing is often considered efficient because it allows organizations to free up resources to focus on innovation and product development. Another potential benefit is that personal information may be better protected in the cloud. Specifically, cloud computing may improve efforts to build privacy protection into technology from the start

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

and the use of better security mechanisms. Cloud computing will enable more flexible IT acquisition and improvements, which may Permit adjustments to procedures based on the sensitivity of the data. Widespread use of the cloud may also encourage Open standards for cloud computing that will establish baseline data security features common across different services and providers. Cloud computing may also allow for better audit trails.

Fig.1 Cloud Computing

If you are considering a cloud service, you should think about how your personal information, and that of your customers, can best be protected. Carefully review the terms of service or contracts, and challenge the provider to meet your needs [11].

A basic approach is the application is to secure the user data before uploading on cloud. In a cloud computing environment, a user's data can also be stored following additional encryption, but if the storage and encryption of a given user's data is performed by the same service provider, the service provider's internal staff (e.g., system administrators and authorized staff) can use their decryption.

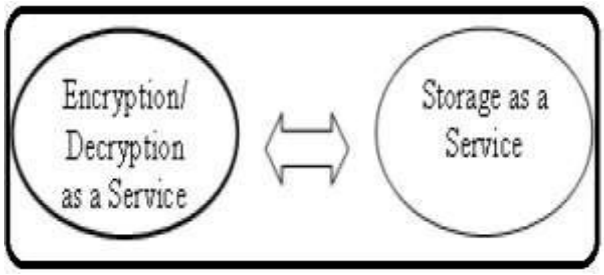

Fig.2 Cloud Services

In this model the data storage cloud system provider is authorized to store the user's encrypted data, but does not have access to the Decryption Key. Thus, the storage system can only retrieve encrypted user data, but is unable to decrypt it. The cloud computing system responsible for encrypting user data has authority over all encryption keys required for data encryption but, given that the encryption provider does not store the user's data, Given that encryption is an independent cloud computing service which is a TPA, a unique feature of the model is that different services are provided by multiple operators. For example, the "Encryption as a Service "provider and the "Storage as a Service" provider cooperate to provide a Cloud Storage System with effective data protection refer fig. 2 [12]

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

II. RELATED WORK

In recent year cloud is very good for storing data. But also some problem are occur to destroy the security. Now a days on clouds various attacks are coming for destroy the security mechanism of cloud computing. Form that we have design some system for protect data on cloud but this all are fail because of their various drawbacks. In previous systems Scenario is First when user want to store data on the Cloud at that time. User was send the confidential data to TPA then TPA will encrypt the data by using some algorithms and then it will send the data to Cloud service provider for storage. As from above approach data was stored in CSP in encrypted format but the drawbacks for the system is that when data was go to TPA, TPA will encrypt the data and send but not delete from there database means TPA can see the User data so the system is fail [12]. Another issue for that When we store data on cloud at that time first of all when user choose data from the user section at that time he will send data to the Security cloud but how can the user can trust on security cloud means if user send the data scloud he can see the all data means also system is fail for that for that issue we make the system strong means used The symmetric key for Both parties User and Security cloud they use the same key for communication from that key they will send data in secure medium. The secure key known as the Deffie Hellman Key for key exchange.
Means when we will transfer the data to user to security cloud user will not trust to security cloud for that user and security cloud generate the same key for communication and from that key he will encrypt data using Blowfish Algorithms for that scenario security cloud cannot hack the data. Also in previous scenario csp (Cloud storage provider) send the file to the user at that moment means Security cloud can hack the data. So for that reason we made the system that user can ask for his file to csp so the system will be strong [12].

III. PROPOSED APPROACH

In our propose approach we remove the drawbacks of previous approach such as, Three different network entities can be identified as follows
User: User is an entity, which has large data files to be stored in the cloud and relies on the cloud for data maintenance and computation, can be either individual consumers or organizations. Also he is totally responsible for storage data.[7][12].
Third Party Auditor (TPA) or security cloud: TPA is an entity, which has expertise and capabilities for Encryption and decryption Service. When client want to store data at the cloud storage at that time TPA (encryption/decryption service) Encrypt the data and return back to user for storage purpose.[7]
Cloud Storage Server (CSS): CSS is an entity which is totally responsible for storage the data. After encrypting your data if you want to store the data on cloud Storage server [7].

In the whole scenario When we user want to store confidential data to cloud for storage. But now a days peoples do not trust on cloud for storage because for leakage of data from cloud. For that we make a system for secure data storage in cloud. For remove the drawbacks for previous model we design this security services when data is encrypted at that nobody can intact the data. This scenario has been divided in A. *Data upload scenario*
First end user login with his user name and password if he is authenticate user at that time by using deffie Hellman[4],[5] key is exchange for that session and user calculate the SHA value for the data for integrity purpose user will calculate the SHA value by using SHA-512 After that user select which data(any file) is to be store on cloud side now user encrypt the data by using DH keys and send to the security cloud(TPA).Now TPA will decrypt data by using DH keys and Encrypt by using AES algorithm[3] and stored the Master key of AES for that user for decryption process and TPA will send Data to the user for store to the storage cloud side and also TPA(security cloud) will delete data from TPA side only stored master key of AES of each user.[12]

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

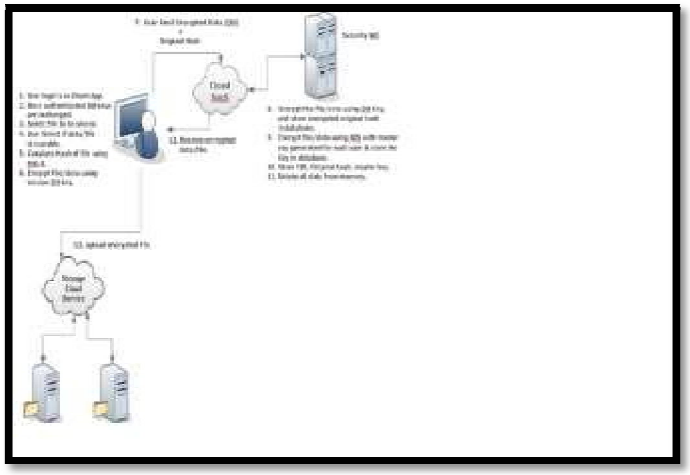

Fig. 3 Data Upload Scenario

B. *Data Download scenario*

Data download scenario is reversed scenario of data upload scenario when user want his data from storage cloud at that time he request to storage cloud for data back once he will get data from storage cloud he want to access the data but the data is in encrypted form for the data decryption process we will have to send data to security cloud. When we send the encrypted data to security cloud it will decrypt the data by using AES [3] Master Key which will be stored in the Security cloud. Again for security purpose TPA will encrypt the data by using DH [4],[5] keys and send to user. At last user will decrypt the data by using DH[4]keys. For check the data integrity User will check the data by using the SHA-512 and he will match the Previous SHA value with this. If the SHA value match your data integrity is good means nobody Hack your data in security cloud as well as Storage cloud [12].

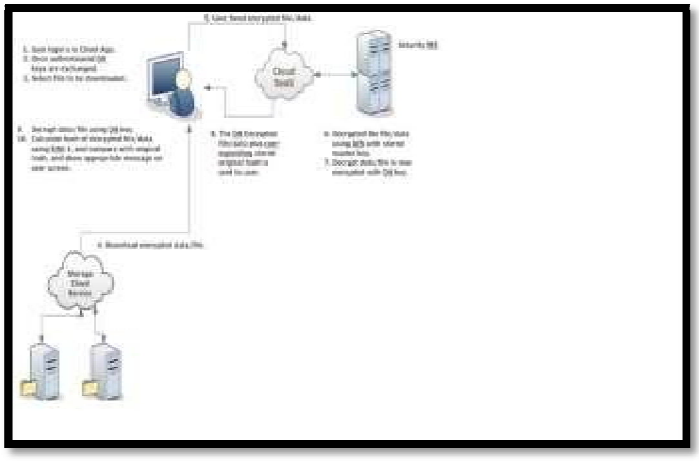

Fig.4 Data Download Scenario

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

IV. WORKING OF PROJECT

The project has the Two Section Upload and Download section
The objective of project cloud is to encrypt and decrypt the user data When user want to upload the data to the cloud side at that time he will not trust on cloud for that reason we make security cloud as a virtual cloud for the encrypt and decrypt the data for user. In that users goal are to be covered. In the whole scenario Security cloud is the main entities.
First the deffie hellman key exchange algorithm is user for to make the shared key between the two parties that is user and security cloud. We have to make the key for encryption between scloud and user.
For that firstly user login want his credentials and one random key for make DF key.

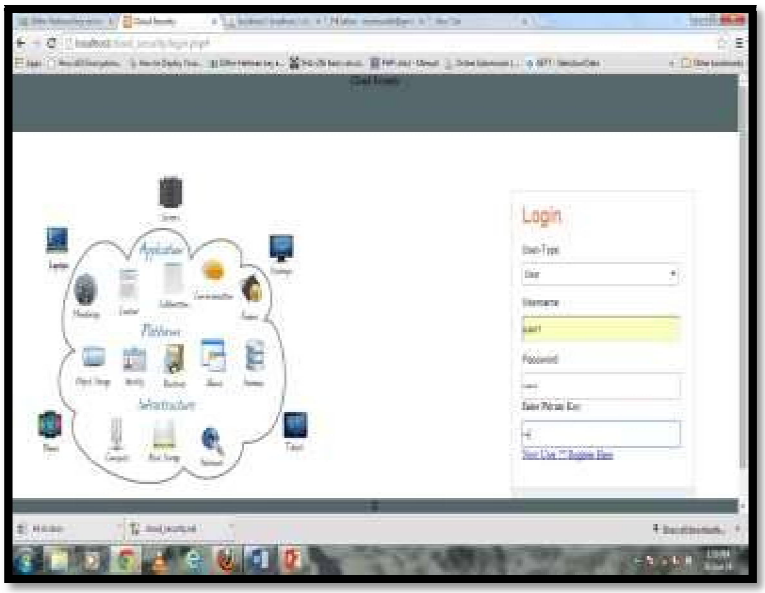

Fig 5 User login

Another Login is the security cloud for encrypt and decrypt the data for users from that scloud can be login for that.

Fig.6 User Portal

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

We here use deffiee hellman Algorithms for key exchange Between two parties means User and scloud.user take one random for key exchange and scloud also take random number for key exchange.
We will see the key exchange algorithms between two parties
Deffie Hellman Algorithm

1. In this Algorithms g and p is constant
2. Suppose g=10 and p=540
3. User choose random number a=5 and calculate
4. $A = g^a \bmod p$
5. Scloud Choose Random number b=7 and calculate $B = g^b \bmod p$
6. Alice and Bob exchange A and B in view of Carl
7. $key_a = B^a \bmod p = 193$(Shared key) $key_b = A^b \bmod p = 193$

When shared key get between two parties user is ready to encrypt data with blowfish and df key

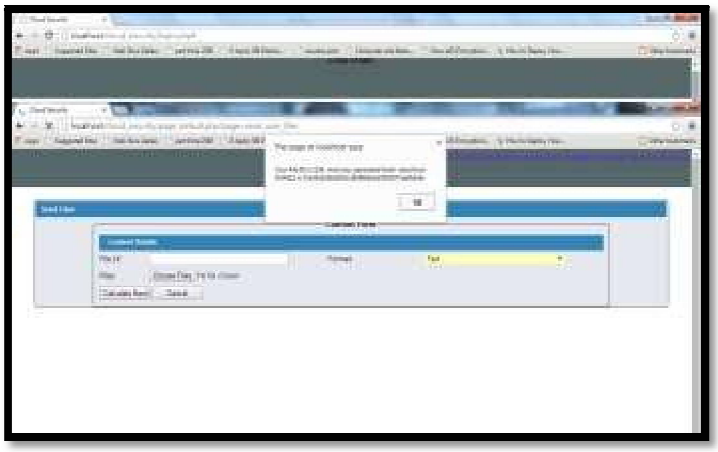

Fig. 7 User Choose file

After choose the file to user he has to calculate with SHA for hashing for intigrty. And then encrypt with blowfish and send to security cloud. When security cloud got the file if he want to access the file at that file he got the encrypted file in blowfish format.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

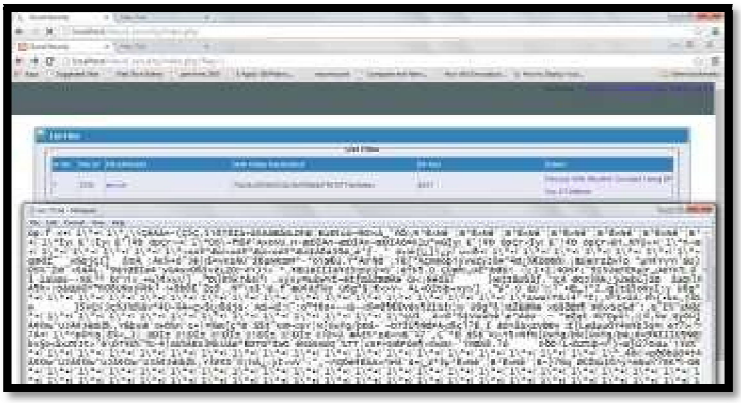

Fig.8 Blowfish Encryption

After got the encrypted file he has to decrypt file with DF key which will be generated by user and scloud side. And then Main duty of Scloud is to encrypt the data by using AES. When Security Cloud will decrypt the file from blowfish and DF key then scloud has to encrypt with AES and Master key is to store in database for Decryption purpose. Again Security cloud want to see that data means do fraurd with Data security cloud he will get encrypted data.

Fig.9 AES Encryption

When AES encryption is do scloud side he will send the file to the user side for upload to the storage cloud.So we will see upto the Upload section and for the download section refer the Download section user first login with their credintials and request for file which will be download from cloud storage sytem once he requsted from cloud storage user will send the file to the security cloud. Security cloud will decrypt the file of AES encryption and encrypt the file with the DF logic and send to the user user will decrypt the file with DF keys and users will get his original file.

V. CONCLUSIONS

Hence this paper gives overall clue of all existing techniques for cloud data security and methods proposed for ensuring data authentication using TPA. , Cloud computing is an emerging commercial infrastructure paradigm that promises to eliminate the need for maintaining expensive computing hardware. We have create new technique which use TPA store

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

encrypted data to cloud, which is hidden from other users. The data will be safe in the public cloud also. In TPM access to keys, data or systems is often protected and requires authentication by presenting a password.
In this application three entities are main User, Scloud as TPA, Cloud Storage service. First user will login and upload the file encrypts with DF key and send to the security cloud. Security cloud will decrypt the file and again encrypt with AES and send to the user for store the storage cloud from that scenario user will very secure for their important data which is highly confidential. so the main role for TPA is to secure their data means encrypt and decrypt the data by using the used proper encryption algorithms After the all process we can calculate the SHA value for file integrity check means when the file coming after download we can check the integrity for that file.An application of Security cloud is to be implemented for encryption and decryption of the user's data. Actually user are very confuse about their data storage on cloud which provider is to use for data storage so for this point of view we will create this application. Now in this scenario user data is very secure.

REFERENCES

[1]Jing-Jang Hwang, Hung-Kai Chuang,Yi-Chang Hsu, Chien-Hsing Wu, "A Business Model for Cloud Computing Based on a Separate Encryption and Decryption Service," Proceedings of the 2011 International Conference on Information Science and Application, April 2011.
[2]Cong Wang, Qian Wang, and Kui Ren, Wenjing Lou," Ensuring Data Storage Security in Cloud Computing"
[3]Avi Kak Lecture 8: AES: The Advanced Encryption Standard Lecture
[4]Notes on "Computer and Network Security" Dieter Gollmann (2006). Computer Security Second Edition West Sussex, England: John Wiley & Sons,Ltd.
[5]Williamson, August 10, 1976. Diffie, W.; Hellman, M. (1976). "New directions in cryptography"(http://www-ee.stanford.edu/%7Ehellman/publications/24.pdf). IEEE Transactions on Information Theory 22 (6):644–654. doi:10.1109/TIT.1976.1055638
Bhavna Makhija, VinitKumar Gupta, Indrajit Rajput,"Enhanced Data
[6]Security in Cloud Computing with Third Party Auditor" proceeding of the , February 2013 International Journal of Advanced Research in Computer Science and Software Engineering.
[7] Qian Wang, Student Member, IEEE, Cong Wang, Student Member, IEEE, Kui Ren, Member, IEEE, Wenjing Lou, Senior Member, IEEE, and Jin Li" Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing
8] John W. Rittinghouse,James F. Ransome © 2010 by Taylor and Francis Group, LLC CRC Press is an imprint of Taylor & Francis Group, an Informa business" Cloud Computing Implementation, Management, and Security" [9]
[10]Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou,‖Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing‖ in IEEE INFOCOM 2010, San Diego, CA, March 2010.
[11]Introduction to Cloud Computing http://www.priv.gc.ca/resource/fs- fi/02_05_d_51_cc_e.pdf
[12] Ankit Mune, Prafull pardhi "Security for cloud computing data using a security cloud as a Third party auditor (TPA): A Survey" in International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 3, March 2014
[13] Ashish Bhagat,Ravi Kant Sahu "Using Third Party Auditor for Cloud Data Security: A Review" International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 3, March 2014