SECURITY STORAGE MODEL OF DATA IN CLOUD

Sonia Arora[1] Pawan Luthra[2]
[1,2]Department of Computer Science & Engineering, SBSSTC
Ferozepur , Punjab, India
Email: [1]soniaarora141@gmail.com, [2]pawanluthra81@gmail.com

Abstract— For IT Enterprise cloud computing has become the new generation architecture. Comparing with traditional computing designs, it provides large data centers to move the application softwares and databases. Cloud computing has attained huge recognition from industries but it still facing many challenges at initial stage which obstructs the growth of cloud. One of the major issue is security of data stored in cloud service provider as cloud has only single security structure but demands of customers are increasing. Therefore this paper focus more on data storage security model of cloud. The data model of default gateway proposed in this paper is focused on providing more security to the platform. This gateway is used to encrypt the data completely with best encryption techniques before sending the data on cloud storage. Maintaining the security during transmission is the major concern, therefore secure OTP is proposed and various hashing techniques are used to sustain the integrity of data.

Index Terms— Cloud Computing, One Time Password, Encryption, Hashing, Integrity

I. INTRODUCTION

Cloud computing is achieving popularity nowadays that aims to provide dynamic scalable resources in computing over the internet as services [1]. The self-service, on-demand, pay per-use, and scalable computing services provided by cloud which reduce capital and operative overheads for hardware and software[2], the concern of securing the data at cloud will also be expand with this. Security issues increases because the data user and the resources to be used by the user are all on the internet and at the remote locations, so the customers cannot have full control on services provided by the service provider. Issues arise when unauthorized person disturbs the data. While moving services to cloud, the data safety at provider's site and data in transmission between host and server must be ensured.
For this to be ascertained, the authentication mechanism on the cloud must be very secure and proper encryption method or algorithm is to be followed to encrypt the data. Also the integrity of data should be sustained using proper hashing method and with all these techniques we can maintain the data security.

Cloud is a means to provide the services to the customers with the least effort from the shared pool of resources. In cloud, the various services available are:

- **Software as a service(Saas):** Provide the consumers the Applications or Services created by Cloud Service Provider(CSP) and which are running on Cloud infrastructure.
- **Platform as a service(Paas):** Provide the consumers with the ability to deploy their applications onto the cloud infrastructure. These applications are created by the consumers using the tools and programming languages provided by the cloud provider. Thus, consumers have control over the deployed applications and possibly environment configurations of applications but not on the underlying cloud infrastructure including server machines(physical or

virtual), storage drives, networks, or operating systems. [3]

- **Infrastructure as a service(Iaas)**: Consumers are provided with the capability to provision storage, networks, processing and other computing resources, also allow the consumer to run arbitrary software, which include operating systems and applications on it.

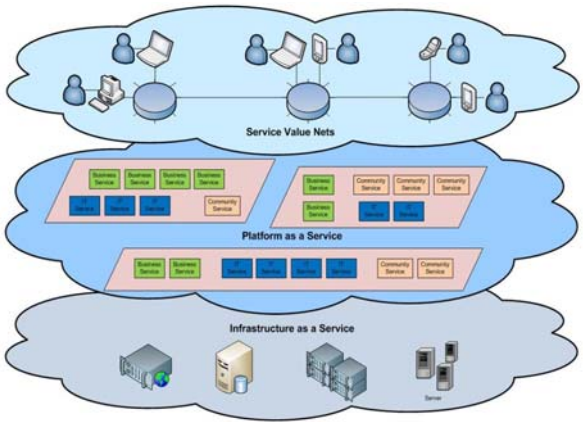

Fig. 1: Services in cloud

Various organizations will have to trust third party to keep their data safe. As cloud is located outside the domain of data owner's, therefore issues of trust between the cloud service provider and data owner will always be there. As data stored in cloud is very confidential and sensitive and it should not be disclosed to unauthorized member [4].

Therefore to maintain trust between cloud service provider and customers, third party auditor act as default gateway which is involved to check the clients data and will enhance more data security to it.

The main objective of this paper is to increase security of data on cloud, discussing the major flaws which were found while maintaining authenticity and integrity of data. The improved data security model and software is implemented to enhance the work in data security of cloud computing based on the study of cloud architecture.

II. RELATED WORK

This section emphasize recent researches in cloud data storage. Kamara et al. [5] discussed about a model for securely storage of data without concerning the components involved for architecture. Wei et al. [6] proposd a SecCloud to achieve security goals. As it jointly considers data storage security and auditing services in cloud, which is very effective and improve efficiency to achieve secure cloud computing. But it is need to be implemented in real platform like EC2 or openstack, also it should focus more on privacy preserving issues. Chow et al. [7] here it more focused on providing secure cloud data storage for dynamic users. It verifies the design with group signature and identity based encryption with constant size cipher texts. It includes confidentiality traceability .

Choudhury et al. [8] proposes a new authentication system for cloud. As in this technique one time password is encrypted using public key of user to obtain encrypted onetime password. It removes dependency on third party but limit is its key size. Fred et al. [9] proposes the Rubbing Encryption Algorithm (REAL) to implement a Mobile-based and a Cloud based OTP Token as design examples which can easily resists the security attacks.
Sood et al. [10] proposed a framework to provide data security to the data. It composed of two phases. Firstly it deals with secure transmission and storage of data in cloud. Second it deals with retrieval of data from cloud. Message authentication code and double authentication with verification of digital signatures are combined to achieve reliability, integrity and availability of data. Patel et al. [11] proposed a model to maintain the computation and communication cost while achieving storage correctness with provision to consider dynamic nature of cloud. Its main role is to develop client application for cloud customer which proved functionalities like encryption-decryption, key management, encoding, decoding, integrity checking functions like MAC, Hash.

Manjusha et al. [12] proposed a multi authority hierarchical attribute based encryption technique which is gives highest security in NIST statistical test compared to key policy and cipher text attribute based encryption techniques. As it preserve major issue of cloud computing which is confidentiality and integrity of data in cloud.

III. SECURITY ISSUES IN CLOUD

Various security concerns are discussed:

- **Data integrity and Reliability**

In cloud computing, anyone from any location can access the data. Cloud does not differentiate between common and sensitive data. Thus, the reliable availability of users data is an important aspect of cloud service.

- **Data Confidentiality**

Confidentiality refers to having the ability to access protected data only by authorized systems or users. As the number of users, devices and applications involved increases, the threat of data compromise on the cloud also increases because number of accessibility increases day by day [13].

- **Multitenancy**

Cloud computing is based on a computing model where resources are shared at host, application and network level. As in multi-tenancy multiple tasks, or processes are shared, this presents a number of privacy and confidentiality issues. [14].

- **Loss of user identity/password**

For an authorized access, authentication is required to be there in the cloud computing security structure. Thus, if the identity and password of the user is lost or is revealed by mistake to any unauthorized person, the data can be at risk [10].

- **Data Tampering**

There is always a concern for data being tampered by unauthorized party. Tampering refers to the data which is entered by user are changed without user's authorization. This is employed by criminals or thieves to intentionally obtain personal or business information about the user.

In Table 1 this shows that there are three types of data in cloud computing. Firstly data in storage, then in transmission, lastly in processing the data.

TABLE I: Data Storage in cloud Computing [15]

Storage	Transmission	Processing
Symmetric encryption	Secret socket layer SSL encryption	Homomophric encryption
AES-DES-3DES-Blowfish- MARS	SSL 1.0-SSL 3.0-SSL 3.1-SSL 3.2	Unpadded RSA- ElGamal ...

IV. METHODOLOGY

Security and trust problem has always been the challenging issue in cloud. Therefore this proposal provides data security model to strengthen security using OTP authentication, encrypting data automatically and checks integrity by using hashing algorithms.

A. Proposed Model

In this model, single default gateway is introduced as a platform to secure sensitive data across multiple cloud applications. In this gateway three phases are implemented as shown in Figure 2.

Proposed data security model is implemented using cloudsim 3.0 using Java language, Mysql-server for storing data in database. It is built in Eclipse IDE 3.8 using Ubuntu 14.04 (32 bit).

B. Implementation Details

1) Phase1(OTP Authentication): Starting with the authentication details:

- Cloud authentication starts with user registration and account is created for particular company.
- Cloud confirms user's registration and user login withhis/her username and password.

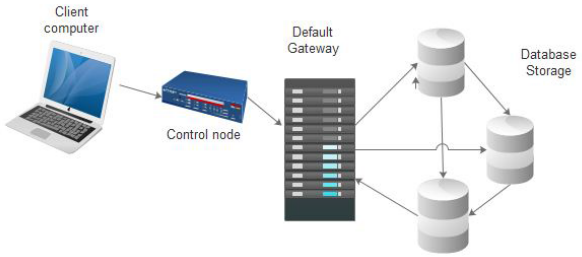

Fig. 2: Default gateway security model

- Checking of valid username and password is performed by cloud provider by searching in DB in cloud storage.

- Cloud provider generates OTP based on information of the client which is stored in OTP temporary DB using MD5 algorithm.
- User of cloud will receive valid OTP through email which will be entered. Validation of OTP is checked by searching in OTP temporary DB. If not valid will display error message.

Flowchart of Login phase with authentication is described in Figure 3.

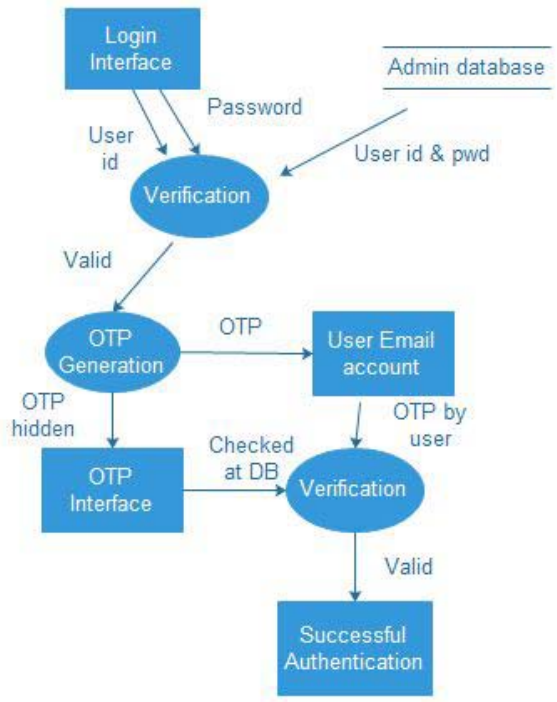

Fig. 3: Login phase with OTP authentication

2) Phase2(Encryption): After login to the cloud, client need to upload the file in cloud but it have to pass through gateway where randomly one algorithm will be chosen from eight algorithms which are RC6, RC4, Blowfish, AES, DES,MARS, Two-Fish,3DES to encrypt the file and then transfer to cloud.

3) Phase3(To check integrity):

- Hash files will be generated in cloud server using MD4, MD5, SHA-1, SHA-2 algorithms.
- Integrity of the data is checked using these hash values.
- Cloud user requests the data, then cloud server decrypts data automatically and will checked the integrity.

Fig. 4: Encryption at default gateway

- If all files of hash codes are matched then file is downloaded at client side, else file is accessed by someone.

V. SIMULATION & RESULTS

This section provides the simulation and results of the proposed structure.

A. Authentication

OTP steps are described in figure 6.

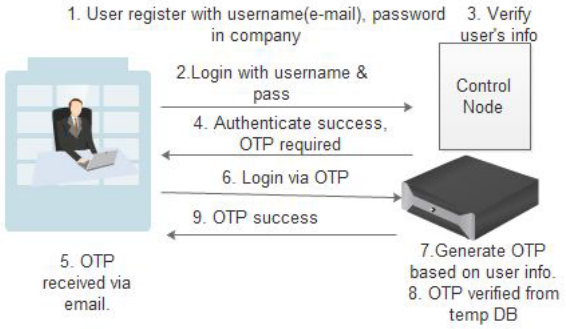

Fig. 5: OTP Authentication steps

The cloud controller generates 1000 OTP using MD5 algorithm based on user's information. Controller saves 1000 OTP in temporary OTP database. Figure 6 shows the Login screen of the proposed software.

Fig. 6: Login screen

User login to cloud website with OTP which is received via e-mail, verifies with the temporary OTP database. If OTP login is valid, login success [16]. If failed then attempt again.

Figure 7. shows the OTP authentication screen of the proposed software.

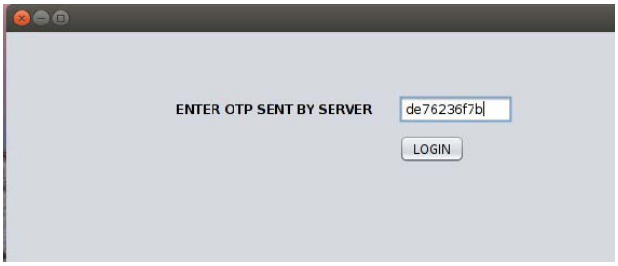

Fig. 7: Proposed OTP screen

1) Benefits of OTP:

- It offers much higher security than static passwords[17].
- OTP's are immune against password sniffing attacks[18].
- Low cost to deploy authentication strongly.
- Protected from unauthorized access.
- It offers two-factor authentication which makes it harder to steal or crack a user information.

B. File Encryption

In proposed software gateway will encrypt the uploaded file with randomly choosing NIST eight modern encryption algorithms namely: RC4, RC6, MARS, AES, DES, 3DES,Two-Fish and Blowfish. Figure 8 shows the Uploading screen:

Fig. 8: Proposed Upload screen

Experiment results shows comparison to indicate the best encryption techniques which enhance security.

Figure 9 indicates time taken by a file in different slots. The results shows the superiority of AES, RC4 followed with Blowfish as they always take less time in encryption/decryption than other algorithms.

C. Ensure Integrity

Integrity is to ensure the data presents are valid and true source of data which also guards against improper modification of information to sustain the authenticity and non-repudiation of information [19].

To solve the trust problem between cloud storage and customer, a simple solution of integrity is proposed to check the integrity of data by producing hash values of the file using MD4, MD5, SHA-1 and SHA-2 algorithms.

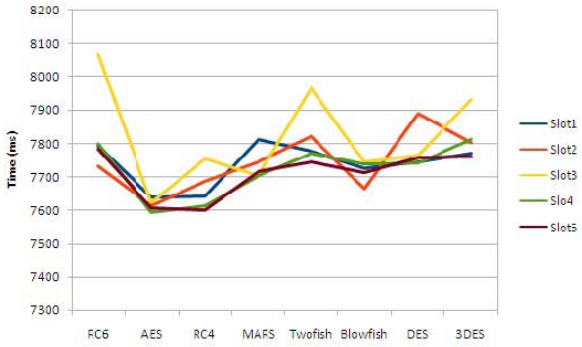

Fig. 9: Encryption/Decryption time of different algorithms

Figure 10 shows that hash values which are produced after uploading the file. When users store data in cloud, server also store four hash values with them.

Fig. 10: Calculate hash values to check integrity

To retrieve the file, server generates new hash values where integrity is checked by comparing the new hash values with the stored hash values.

If hash values not matched then software give message of hash values change like in figure 11:

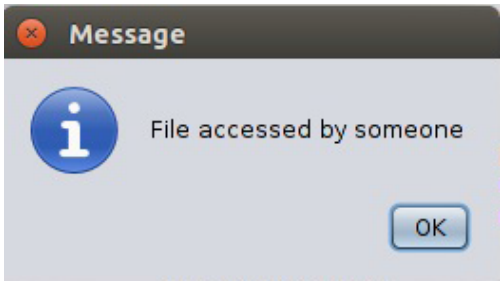

Fig. 11: File accessed

Following are benefits of using this efficacy:

- Not much effort required in implementation.
- Time required to compute the hash values is not much.
- Security level can be change flexibly.
- Space required to store hash values is not much.

VI. CONCLUSION

Security and trust has always been the major issue in cloud computing. This paper points the security constraints and how to overcome these issues. Here the security model is proposed which attempts to focus on providing security at cloud side.

In this OTP (One-Time Password) is provided which shows two-factor authentication software. Default gateway is proposed where randomly encryption algorithms is chosen, results shows that the AES, RC4 and followed by Blowfish are best algorithms as they always take less time to encrypt/decrypt.

In addition to this data integrity is ensured by using hash algorithms. The summarized results of proposed security model of data is in Table 2:

TABLE II: Summarized Results of proposed data security model

Features	Description
Authentication	Mathematically generated OTP authentication
Provide Encryption	File is encrypted randomly chosing one algorithm from eight algorithms.
Best Encryption algorithm	AES, RC4 and Blowfish are best among them.
Data integrity	Hashing- MD5- MD4-SHA-1-SHA-2

ACKNOWLEDGMENT

The authors would like to thank the editors and the anonymous referees for their valuable comments and suggestions.

REFERENCES

[1] A. K. Dubey, A. K. Dubey, M. Namdev, and S. S. Shrivastava, “Cloud user security based on rsa and md5 algorithm for resource attestationand sharing in java environment,” in Software Engineering (CONSEG),2012 CSI Sixth International Conference on. IEEE, 2012, pp. 1–8.

[2] J.-M. Bohli, N. Gruschka, M. Jensen, L. L. Iacono, and N. Marnau, “Security and privacy-enhancing multicloud architectures,” Dependable and Secure Computing, IEEE Transactions on, vol. 10, no. 4, pp. 212–224, 2013.

[3] V. Paranjape and V. Pandey, “An approach towards security in private cloud using otp.”

[4] G. B. Selman Haxhijaha and F. Prekazi, “Data integrity check using hash functions in cloud environment,” 2014.

[5] S. Kamara and K. Lauter, “Cryptographic cloud storage,” in Financial Cryptography and Data Security. Springer, 2010, pp. 136–149.

[6] L. Wei, H. Zhu, Z. Cao, X. Dong, W. Jia, Y. Chen, and A. V. Vasilakos, “Security and privacy for storage and computation in cloud computing,” Information Sciences, vol. 258, pp. 371–386, 2014.

[7] S. S. Chow, C.-K. Chu, X. Huang, J. Zhou, and R. H. Deng, “Dynamic

[7] S. S. Chow, C.-K. Chu, X. Huang, J. Zhou, and R. H. Deng, “Dynamic secure cloud storage with provenance,” in Cryptography and Security: From Theory to Applications. Springer, 2012, pp. 442–464. secure cloud storage with provenance,” in Cryptography and Security:From Theory to Applications. Springer, 2012, pp. 442–464.

[8] G. Choudhury and J. Abudin, “Modified secure two way authentication system in cloud computing using encrypted one time password.” International Journal of Computer Science & Information Technologies, vol. 5, no. 3, 2014.

[9] F. Cheng, “Security attack safe mobile and cloud-based one-time password tokens using rubbing encryption algorithm,” Mobile Networks and Applications, vol. 16, no. 3, pp. 304–336, 2011.

[10] S. K. Sood, “A combined approach to ensure data security in cloud computing,” Journal of Network and Computer Applications, vol. 35, no. 6, pp. 1831–1838, 2012.

[11] H. B. Patel, D. R. Patel, B. Borisaniya, and A. Patel, "Data storage security model for cloud computing," pp. 37–45, 2012.
[12] R. Manjusha and R. Ramachandran, "Comparative study of attribute based encryption techniques in cloud computing," in Embedded Systems (ICES), 2014 International Conference on. IEEE, 2014, pp. 116–120.
[13] D. Zissis and D. Lekkas, "Addressing cloud computing security issues,"Future Generation computer systems, vol. 28, no. 3, pp. 583–592, 2012.
[14] C. Alliance, "Security guidance for critical areas of focus in cloud computing v3. 0," Cloud Security Alliance, 2011.
[15] E. M. Mohamed, H. S. Abdelkader, and S. El-Etriby, "Enhanced data security model for cloud computing," in Informatics and Systems (INFOS), 2012 8th International Conference on. IEEE, 2012, pp. CC–12.
[16] E. M Mohamed, H. S Abdelkader, and S. El-Etriby, "Data security model for cloud computing," in ICN 2013, The Twelfth International Conference on Networks, 2013, pp. 66–74.
[17] V. Paranjape and V. Pandey, "An improved authentication technique with otp in cloud computing," International Journal of Scientific Research in Computer Science and Engineering, vol. 1, no. 03, pp. 22–26, 2013.
[18] I. Das and R. Das, "Mobile security (otp) by cloud computing."
[19] H.-S. Yu, Y. E. Gelogo, and K. J. Kim, "Securing data storage in cloud computing," Journal of Security Engineering 9th March, 2012.