JCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-6, Issue-8, Aug 2018 E-ISSN: 2347-2693

Security Approach for Data Storage and Retrival in The Cloud

Somnath Basak[1*], Somnath Dey[2], Mrinmay Deb [3]

[1,2,3]Department of Computer Science & Engineering, Brainware Group of Institutions, Kolkata, India

**Corresponding Author: somnathbasak30@gmail.com, Tel.: +91-98300-25305*

Available online at: www.ijcseonline.org

Accepted: 14/Aug/2018, Published: 31/Aug/2018

Abstract— Since the beginning of courtesy, man has always been motivated by the need to make advancement and better the existing technologies. This has led to remarkable development and progress which has been a launching pad for further evoluation of all the momemtous advances made by society from the beginning till date. Cloud computing is the concept of using outlying services through a network using various resources. It is basically meant to give maximum with the minimum resources i.e. the user end is having the minimum hardware requirement but is using the maximum capability of computing. This is possible only through this technology which requires and utilizes its resources in the best way. But this advantage comes at a cost. Firstly, the data is uploaded insecurely which has a high risk of being hacked by some malicious people. Secondly, the data saved at outlying servers is under the surveillance of unauthorized people who can do anything with our data and Information. So, these data security risks are causing a barrier in the development of the area of cloud computing infrastructure. In this paper we have discussed about the various techniques by which we can enhance the cloud service in relation to security and data privacy and also designed a new effective cloud data security infrastructure.

Keywords—Cloud Computing, OTP, Data Security, Data Privacy.

I. Introduction

Organizations today are progressively looking towards Cloud Computing as a new radical technology encouraging to cut the cost of development and still produce highly reliable and flexible services. The Cloud technology is a flourishing trend and is still experience lots of observation.

Cloud computing usually associate the relocation, storage, and prepare of information on the 'providers' framework, which is not included in the 'customers' control policy. The concept Cloud Computing is linked closely with those of Information as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS) all of which means a service-oriented architecture. In the cloud, the end user is just using a very light device which is capable of using a network that connects it to a server at some other location. The users do not need to store the data at its end as all the data is stored on the remote server at some other place. So, there is a need to protect the data against unauthorized access, modification or denial of services, data loss and data integrity problem.

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. [1]

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.

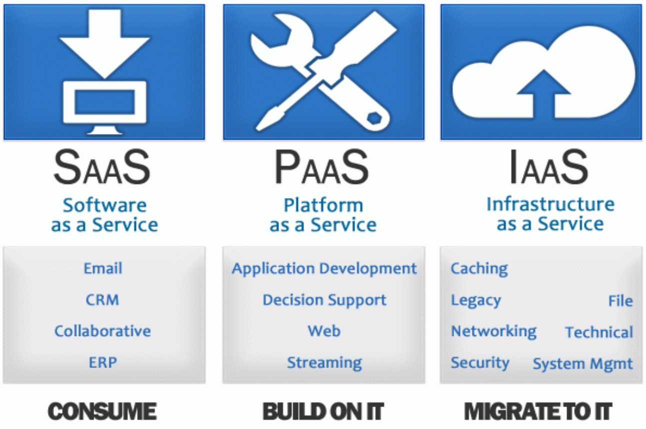

Figure 1. Different cloud services

This paper is organised in 5 different sections. In section I the introduction is given, section II illustrates the related works which act as a motivation for our proposed work. In section III, the proposed work is defined briefly along with implementation. In section IV the results are represented that are obtained after implementing the proposed work. In last section V the study concludes briefly on the basis of the obtained results and highlights the future work.

II. Related Work

IT Enterprise cloud computing has become the new generation architecture. Comparing with traditional computing designs, it provides large data centers to move the application software 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 issues is security of data stored in cloud service provider as cloud has only single security structure but demands of customers are increasing [2]. Therefore, this paper focuses 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.

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 [3].

Therefore, to maintain trust between cloud service provider and customers, third party auditor acts as default gateway which is involved to check the client's 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.

This section emphasizes recent researches in cloud data storage. Kamara et al. [4] discussed about a model for securely storage of data without concerning the components involved for architecture. Wei et al. proposed 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 open stack; also, it should focus more on privacy preserving issues. Chow et al. here it more focused on providing secure cloud data storage for dynamic users [5]. It verifies the design with group signature and identity-based encryption with constant size cipher texts. It includes confidentiality traceability.

Choudhury et al. [5] 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. 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. [6] 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. 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. [7] proposed a multi authority hierarchical attribute-based encryption technique which gives highest security in NIST statistical test compared to key policy and cipher text attribute-based encryption techniques. As it preserves major issue of cloud computing which is confidentiality and integrity of data in cloud.

V. Spoorthy et al. [8] make a survey on data storage and security in cloud computing and mainly focus on aspects for providing security for data storage in cloud, also architecture for data storage that are implemented by other service providers vendors in cloud, key points for proving security for data storage.

III. 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.
In our proposed model there will be three phases:

[1]. Authentication process

- System authentication starts with user registration and account is created for particular user.
- System confirms user's registration and user login with his/her username and password.
- System generates OTP based on information of the client which is stored in OTP temporary database.
- User will receive valid OTP through email which will be entered.
- Validation of OTP is checked by searching in OTP temporary DB. If password match user will allow accessing the system. If not valid will display error message.

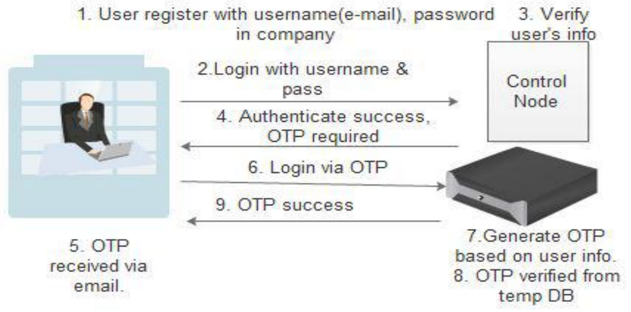
1. User register with username(e-mail), password in company
3. Verify user's info
Control Node
2.Login with username & pass
4. Authenticate success, OTP required
6. Login via OTP
9. OTP success
5. OTP received via email.
7.Generate OTP based on user info.
8. OTP verified from temp DB

Figure 2. OTP Authentication Steps

[2]. Encryption of user data: [Time of Data Upload]

- After login to the system, client need to upload the file in file storage but it has to pass through gateway where randomly one algorithm will be chosen from the algorithms AES, DES, 3DES, Blowfish to encrypt the file and then transfer to cloud storage. The user needs to give the encryption key. (The encryption key is treated as a password in purpose)

[3]. Decryption of user data: [Time of Data Download]

- User authentication process are same as time of data upload.
- If authentication process is succeeded then user chose the same key as password to decrypt (download) the data from storage. (All three algorithms are symmetric key algorithm)

For the security purpose we need to use the three cryptographic algorithms for the encryption and decryption of file. So, the algorithms like AES, DES, 3DES, Blowfish and the implemented Java code of that algorithm are the major important information requirements. Also, some information about the working principle to deal with the file storage is required.

For the development of the proposed system Java programming language and MySQL database server has been used.

IV. Results and Discussion

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

A. Authentication

The cloud controller generates 5000 OTP using MD5 algorithm based on user's information. Controller saves 5000 OTP in temporary OTP database. 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. If failed then attempt again.

B. File Encryption

In proposed software gateway will encrypt the uploaded file with randomly choosing NIST modern encryption algorithms namely: AES, DES, 3DES, Blowfish.
Experiment results shows comparison to indicate the best encryption techniques which enhance security.

Table 1 indicates time taken by a file in different slots. The results show the superiority of AES followed with Blowfish as they always take less time in encryption/decryption than other algorithms.

Table 1. Comparison of different algorithm

Algorithm	**Block Size (Bits)**	**Key Size (Bits)**	**Speed**	**Throughput (megabytes/sec)**	**Security**
DES	64	56	Low	4.01	Less
3DES	128	112,168	Low	3.45	Less
AES	128	128,192, 256	Fast	4.174	More Secure
Blowfish	64	32-448	Fast	25.892	More Secure

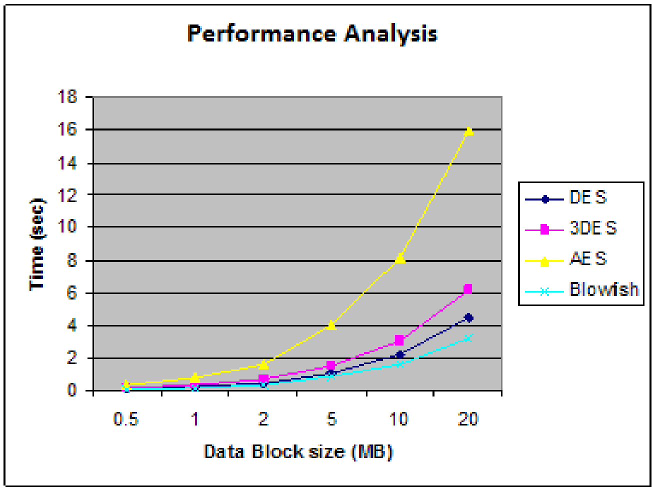

Figure-3

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 [10]. To retrieve the file, server generates new hash values where integrity is checked by comparing the new hash values with the stored hash values [9].

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.

V. CONCLUSION AND FUTURE SCOPE

The main objective of the paper is to provide a security infrastructure and for providing the secure infrastructure the process of encryption is the main key. Whenever a user will upload a file to the file storage the raw data will not be directly stored in the storage. During this uploading one among the four-cryptography algorithm will be called randomly and the user need to provide a password as a key with the file. This password will work as the key for the encryption. For this reason, at the time of downloading the file the user need to give the password again associated with that file. This password will again work as the key for the decryption of the file.

To use the whole system, the user need to register himself/herself to create an account. And also, during the login process each time the user need to go through an authentication process. The authentication process is generally accomplished by generating OTP.

In today's era demand of cloud is increasing so the security of the cloud and user is on top concern. Hence, this algorithm is helpful for today's requirement. In future we may develop some hybrid encryption algorithm which executes in much less time rather than the traditional algorithms that we used in this paper and also provides high security infrastructures.

REFERENCES

[1] V. Paranjape, V. Pandey, "An approach towards security in private cloud using otp", International Journal of Emerging Technology and Advanced Engineering (IJETAE), Vol.3, Issue.3, pp.683-687, 2013.

[2] S. Arora, P. Luthra "*Security Storage Model of Data in Cloud*", International Journal of Current Engineering and Scientific Research (IJCESR), Vol.2, Issue.6, pp.99-105, 2015.

[3] H. B. Patel, D. R. Patel, B. Borisaniya, A. Patel, "Data storage security model for cloud computing", Advances in Communication, Network, and Computing, CNC 2012, pp. 37–45, 2012.

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

[5] G. Choudhury, J. Abudin, "Modified secure two-way authentication system in cloud computing using encrypted one-time password." International Journal of Computer Science & Information Technologies, IJCSIT, Vol.5, no. 3, 2014.

[6] 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.

[7] R. Manjusha, R. Ramachandran, "Comparative study of attribute-based encryption techniques in cloud computing", in Embedded Systems (ICES), International Conference on. IEEE, pp.116–120, 2014.

[8] V. Spoorthy, M. Mamatha, B. Santhosh Kumar, "A survey on data storage and security in cloud computing", International Journal of Computer Science and Mobile Computing, IJCSMC, vol.3, Issue.6, pp. 306-316, 2014.

[9] N. Gowtham Kumar, K. Praveen Kumar Rao, "Hash Based Approach for Providing Privacy and Integrity in Cloud Data Storage using Digital Signatures", International Journal of Computer Science and Information Technologies, IJCSIT, Vol.5, pp. 8074-8078, 2014.

[10] E. M. Mohamed, H. S. Abdelkader, S. El-Etriby, "Data Security Model for Cloud Computing", Journal of Communication and Computer, Vol.10, pp.1047-1062, 2013.

Authors Profile

Mr. Somnath Basak pursed Master of Technology from Birla Institute of Technology, India in 2014. He is currently working as Assistant Professor in Department of Computer Science & Engineering, Brainware Group of Institutions, India since 2011. His main research work focuses on Cryptography Algorithms, Network Security, Cloud Security and Privacy, IoT. He has 12 years of teaching experience.

Mr Somnath Dey pursed Master of Technology from University of Calcutta, India in year 2010. He is currently pursuing Ph.D. and currently working as Assistant Professor in Department of Computer Science &

Engineering, Brainware Group of Institutions, India since 2011. His main research work focuses on Cryptography Algorithms, Network Security, Cloud Security and Privacy, Big Data Analytics. He has 10 years of teaching experience.

Mr Mrinmay Deb pursed Master of Science in Information Technology, in the year of 2013. He is currently working as Teaching Assistant in Department of Computer Science & Engineering, Brainware Group of Institutions, India since 2013. His main research work focuses on real-time programming, DJ: Dynamic Adaptive Programming in Java, Internet of Things, IT for support environment, Modular Checking of C Programs with Bounded Model Checker. He has 8 years of teaching experience.