ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

A Survey on an Innovative Method for Providing Maximum Security to the User Data Uploaded On Cloud

Pooja Ambadas Motekar[1], Prof. L.M.R.J. Lobo[2]

P.G Student, Department of CSE, WIT, Solapur University, Solapur, India[1]

Associate Professor, Department of CSE, WIT, Solapur University, Solapur, India[2]

ABSTRACT: Now day's data security on cloud is a major issue for the user who store the data on a cloud. Some cloud service providers take different charges from the users to provide additional security for data. We can provide security guarantees on authentication and on the files over the cloud using various methodologies. It is also necessary to verify a user at each time while providing the file to a user. This proposed paper focuses on the mechanisms like two fish Algorithm for encryption and Decryption purpose, Time based onetime-password Algorithm is using for user authentication and file authentication can be done using an AES algorithm embedding the concept of key management entitled z key distribution. By using the combination of these entire algorithms Authentication will be done. This provides security for the data stored on cloud which is outsourced.

KEYWORDS: Cloud Security, Cloud Service Provider, Advance Encryption Standard (AES), Quantum key Distribution (QKD), Two-Fish.

I. INTRODUCTION

Cloud computing is something which is based on a business model where resources are shared i.e. multiple users are using the same resources at the network level, application level and host level. Multitenancy, one of the cloud computing attribute in cloud computing provides security. It provides a facility for the cloud actors i.e. cloud service providers, tenants and tenants customers, it is also necessary for the governments and regulators. Most of the customers are concerned about the data protection which is access control, encryption, User verification and integrity. In cloud computing a user is enabled to increase as well as decrease their computing resources as needed. They can also release the resources for other users when their work is completed. In the cloud scenario there are some services providers that take charges for the services they provide. A user has to pay only for the Resources which are used and only for the time they require them. Cloud computing also provides the self-provisioning of the resources such as software, storage, and infrastructure.

A.APPLICATIONS OF CLOUD COMPUTING:

In cloud computing there are many applications in all fields such as social networking, business, education field, data storage, entertainment, management, global positioning system and art. Some of the Application that require a Cloud are:MailChimp,GoogleAppsforbusiness,QuickBooks,Gmail,y-mail,BOX.com,Mozy,Joukuu,Toggl,Outright, Facebook,Twitter,Audio box.fm,Moo.

Cloud computing is an emerging technology which has to face many different challenges in various aspects such as data and information handling. The challenges such as security and privacy, provider data and its security, portability, Interoperability, Computing Performance, Reliability and Availability. Now day's data security on cloud is a major issue for the user who store the data on a cloud. Some cloud service providers takes different charges from the users to provide additional security for data. We can provide security guarantees on authentication and on the files over the cloud using various methodologies. It is also necessary to verify a user at each time while providing the file to a user. It is necessary to protect the sensitive data from unauthorized parties. This approaches focuses on the mechanisms like two fish Algorithm for encryption and Decryption purpose, Time based onetime-password Algorithm is using for user authentication as well as authorization, file authentication can be done using an AES algorithm embedding the concept of key management entitled quantum key distribution. By using the combination of these entire algorithms Authentication will be done. This provides security for the data stored on cloud which is outsourced. Data which is present at cloud also hide from the unauthorized parties.

B. BASIC CONCEPTS:

Cloud computing consist of certain models and services which plays the most important role in the cloud environment that perform feasible and better accessible to the end user. Working models for the cloud computing are explained below.

- Cloud Deployment Models
- Cloud Services Delivery Model

1.2.1 Cloud Deployment Model

A Cloud deployment model may be Private, Public, Hybrid and Community in nature.

1.2.1.1 Private Clouds

The private cloud is one which allows the services and system to be accessible which are present inside the organization. The cloud operation can be handled by the single organization. Private cloud, also called as internal cloud has its operations not available to the general public [14].

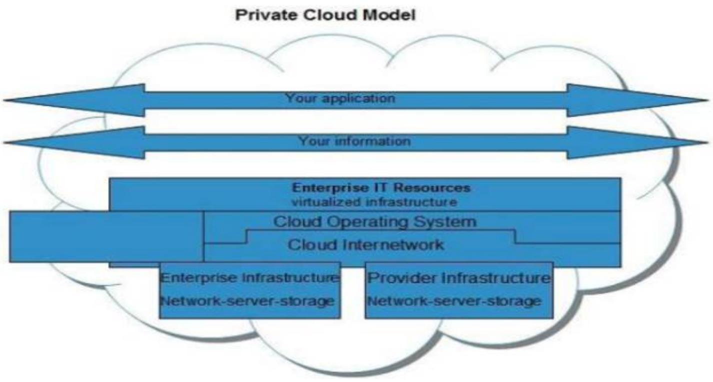

Fig.1.Private cloud computing model

1.2.1.2 Public Clouds

The pubic cloud allows the services and system to be accessible to general public. It is also called as external cloud. Public cloud shares the resources with more numbers of customers so the cost decreases. It provides reliability, Flexibility and Location Independence. Public cloud is managed by a third party from number of data centers [14].

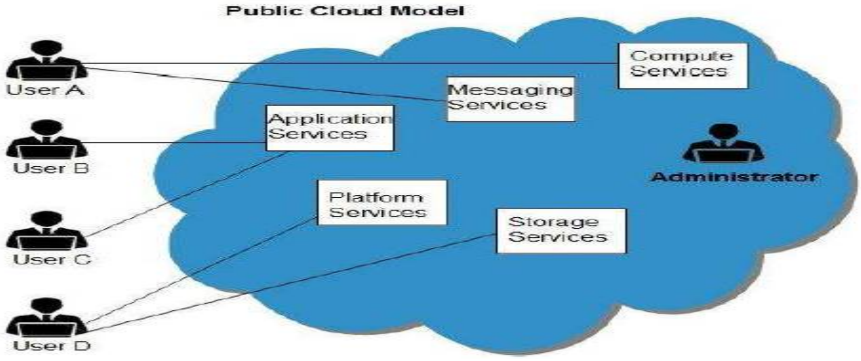

Fig.2.Public cloud computing model

1.2.1.3 Hybrid Clouds

A hybrid cloud is the combination of private and public cloud. There are many advantages of using a hybrid cloud such as it gives the features of both the private and public cloud i.e. scalability. It also provides highest security [14].

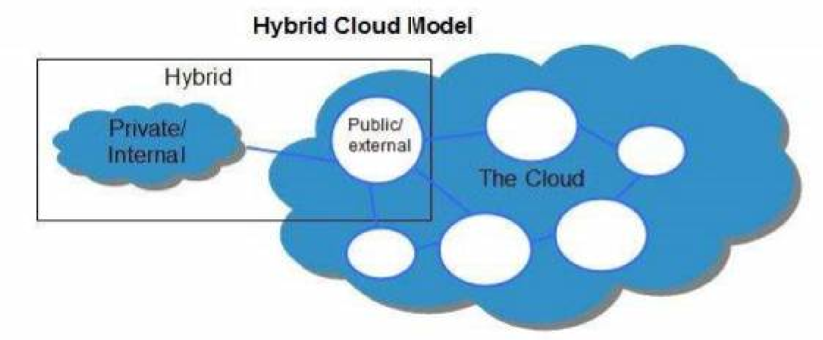

Fig.3.Hybrid cloud model

1.2.1.4 Community Clouds

A community cloud allows services and system to be accessible to the group of organization. Community cloud is used to share the infrastructure between different groups of organization. It provides more security as compare to public cloud [14].

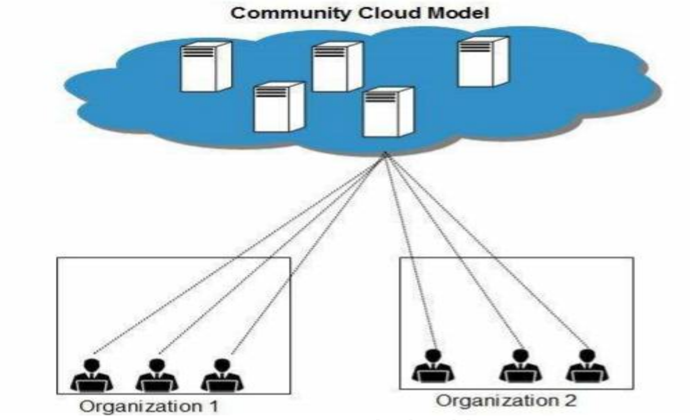

Fig.4.Community cloud model

1.2.2 Cloud Services Delivery Model

The model works on three dimensions Software-as-a-Service, Platform-as-a-Service and Infrastructure -as-a-Service.

1.2.2.1 The Software-As-a-Service Model

In software-as-a-service model (SaaS), the customers who wish to use software need not purchase it, instead he will take software as a pay-per-use model.

1.2.2.2 The Platform-As-a Service Model

In platform-as-a-service model (PaaS), the service provider offers development environment. By using the development environment the application developer is able to develop an application. The provider takes charges for providing the platform.

1.2.2.3 The Infrastructure-As-a-Service Model

It provides access to many fundamental resources such as physical computing resources, location, data partitioning, security, scaling and so on.

C. WE PROPOSED THE SYSTEM WILL HAVE THE FOLLOWING CONTRIBUTIONS.

In our proposed system aim is to Provide Maximum Security to the User data Stored and uploaded on cloud network. We are going to implement three layer Encryption Technique for access Authentication, file/data Security and random key generation factor. This Proposed work focuses on the mechanism of two fish Algorithm for encryption and Decryption purpose, Time based onetime-password Algorithm using for user authentication and file authentication can be done using a AES algorithm embedding the concept of key management entitled quantum key distribution.The aim of this work is to provide file access permission to the user basis on their roles and allowed by Administrator. We also provide data security without any cost. We also maintain file access user log and provide Hash map technique to store the data on a server and Data leakages and security alarm has been provide to user to specify more data security.

1) GPS Location Based
2) IP Restriction over the Network (Fixed IP address)
3) TOTP-At the time of user Login and Downloading
4) Encrypted Email
5) Log maintain- we also maintain file access user log
6) Data leakage
7) Security alarm has been provide to user to specify more data Security

II. Related work

Nikhil Gajra, Shamsuddin S. Khan, Pradnya Rane [1] focused, on the security for the application which is most important connection as we now outsource the storage of possibly sensitive data to third parties. The most important risk too many applications are at the human level. It has been assumed that with sharing of services comes high level of trust. But there are risks that a friend or neighbor may decide to abuse the trust that we are shown on friend or neighbor and they will hack the services that is provided to the user and personalized content. There is some mechanism which protects better security on authentication, but to avoid the risk which is at human level there should be approaches which provide security guarantees on authentication and on the files over the cloud. The approaches consist of Advance Encryption Standard, Blowfish which is used for encryption purpose and the key management and authentication done by using the concept of Elliptic Curve Cryptography.

Rajan.S.Jamgekar, Geeta Shantanu Joshi [2], introduced secure RSA for secure file transmission. They presented a modified RSA algorithm for secure file transmission.

Cong Wang, Qian Wang, and KuiRen, Wenjing Lou [3] focused on data storage security in cloud which is the most important characteristic to consider as a quality of service. To ensure the correctness in the data of the users which is in cloud they told an Effective as well as flexible distributed scheme. By putting into service the homomorphic token with the combination of distributed verification of the erasure-coded data with their scheme to gain with effort of storage correctness protection against future loss and data error localization, i.e., the identification of server who misbehaving. The most prior works, the new scheme further supports secure and data blocks which should be efficient for dynamic operations, which include data update, delete and append. The proposed scheme analysis shows that at a high rate it is efficient as well as rebound readily against byzantine failure for the reason of its Extensive security and performance, malicious data modification attack, and even server colluding attacks.

Slawomir Grzonkowski and Peter M. Corcoran [4] developed a user centric approach to authentication for home networks. A zero-knowledge-proof (ZKP) authentication was used to support the rising generation of cloud infrastructure which allow user to temporarily transfer their service and content rights to the trusted area that is friend's home. This approach enabled sharing of personalized content. A design which is necessity for authentication protocols which uses a zero-knowledge proof (ZKP) technique was developed, allowing the use of a simple user/password authentication.

Patel Megha, Prof.Arvind Meniya [5], remark that anyone who has internet can access cloud services. Now day's cloud computing system with ease can be hacked by different cyber attacks, for this kind of attack Intrusion detection system (IDS) can be emplaced as strong defensive mechanism. In their paper they implemented a new algorithm which stops those DDOS attack. Now day in cloud security the serious thread exists that is Distributed Denial of Service Attack (DDOS).The basic idea behind the proposed system is used to give the security the web server which consists of huge volume of DDOS request when an attack occurs. Sherin Jobe, VenifaMini.G and Jeya A.Celin J [6] remark that in a cloud computing Anonymous authentication there is a technique that is capable to the user to prove that without disclosing real identities In that many existing anonymous authentication protocols assume absolute trust to the cloud provider who stores all private keys. Because of this trust which result in very danger security as well as privacy issues for the cloud provider. The proposed work secure and efficient anonymous mutual authentication protocols using Radio Frequency Identification which is the technology implemented based on ZKP for the cloud services.

Jadapalli Nandini, Ramireddy Navateja Reddy [7] represent many techniques that are used for the elimination of duplicate copies of repeating data, from that technique, the most important technique is data duplication which is the data compression technique. There are many data duplication advantages that are used to reduce the amount of storage space and save the bandwidth when using in cloud storage. In this paper they used many techniques like De-duplication, authorized duplicate check, hybrid cloud confidentiality, encryption technologies.

Volker Fusenig and Ayush Sharma [8] exhibit a new approach called cloud networking. It adds the functionalities of networking to the cloud computing and which also enables dynamic and flexible placement of virtual resources crossing provider borders. This allows different category of optimization, e.g. network load. However, this approach introduces new security challenges. The paper presents a security architecture which is used to define the requirement of the security for the capable to the user.

Nimi P Baby, Dr Salaja Silas [9] present different methodologies which provide privacy as well as security that are studied and are compared based on the need for the cloud computing environment. There are Attribute Based Encryption, Privacy, Key distribution, PRE encryption. One of the major issues in cloud computing is privacy and security of data. This paper survey on different mechanisms used to provide security and privacy for the data in cloud storage system. In today's world Cryptographic methods are widely used for security and along with that biometric and many other solutions are referred. The study and comparison of some methods based on the parameters such as revocation method, bandwidth, granularity, need for third party etc is done in this paper and listed with advantages and limitations of each of them.

Ranjana Badre [10] shows how in cloud computing the large scale of outsourced can be secure as well as the efficient access is provided, data is an important issue. In this paper, a mechanism FADE, a secure overlay cloud storage system, which gives the guarantee, assured file deletion, the improved access control for outsourced data is proposed. The fade architecture is explained in this given paper. Then extensions to FADE are given. The FADE which is extended which is meant for enforcing the outsourced data for security in cloud, which provide the guarantees Access control as well as the Assured deletion to the data stored on the third party cloud.

Prassanna.J, Punitha.K, Neelanarayanan.V [11] have analysed the mechanism for data Accountability and auditing of cloud user data in the distribute cloud. In this context they have analysed an innovative mechanism that technically as well as the data access which is stored in cloud is systematically logging to any data untidily with well supported auditing mechanism.

N. Mahesh Kumar [12] is a survey of different algorithms used in different auditing mechanisms. This is considered as a data environment in cloud that is used for the storage correctness. There are various challenges which need to be addressed for making cloud computing most is accomplishes well in the real life. The challenges like security issues and storage issues are important for the service providers to improve the services. In this paper they have presented different algorithms in auditing services to gain with effort of the data access control which is in cloud and which provides the privacy outsourced data in the cloud environment. They also provided the brief description about the auditing process in cloud for future development.

Sunita Rani, Ambrish Gangal[13] has proposed a hybrid algorithm which is an encryption technique which provides privacy in the cloud. Their analysis fully make a delivery of merging the most important aspects of dynamic and static testing into a tightly interwoven approach for increasing fastest analysis for the security vulnerabilities in software.

III. METHODOLOGY

A. PROPOSED SYSTEM ARCHITECTURE

The Architecture of the system consists of blocks that follow the procedural steps given below for the sender side:

1) Register and Enter Login Information.
2) Generate the OPT and send it to the mobile and email then verify OTP.
3) Check allowed IP Details and verify.
4) Select a file which wants to upload.
5) Generate random key by using Quantum key Generation.
6) Apply AES on key which will generate Encrypted key.
7) Apply AES and Two-Fish on file.

DOI: 10.15680/IJIRCCE.2016. 0409114

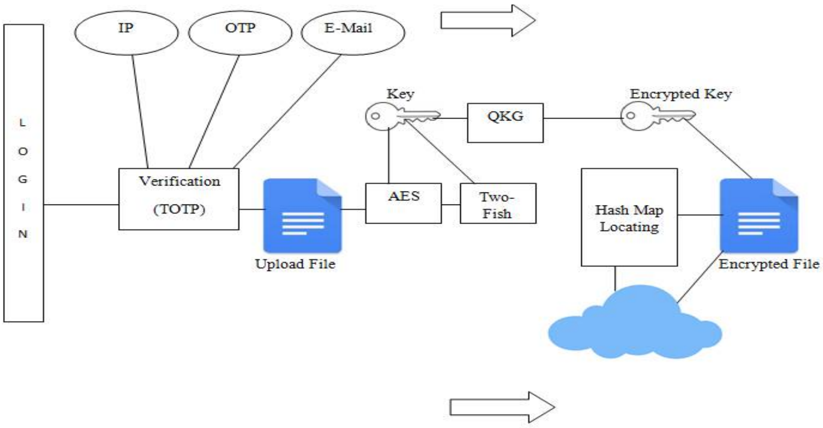

Fig.5.Sender System Architecture(Encryption Process)

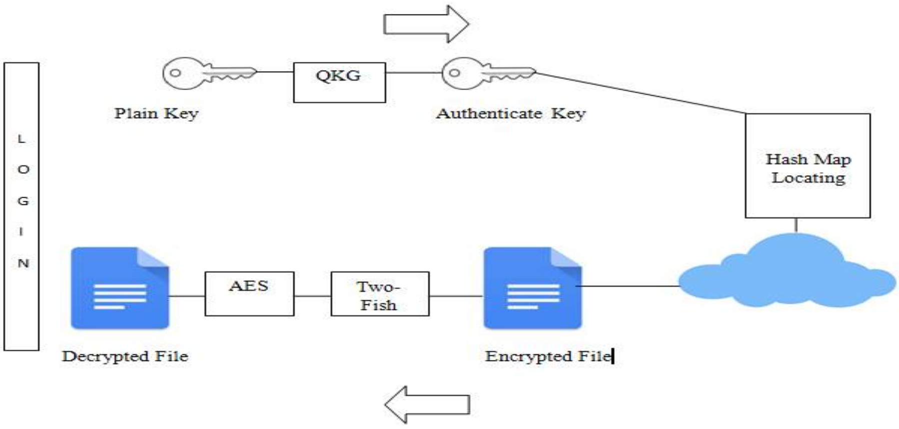

Fig.6.Receiver’s System Architecture(Decryption Process)

The Architecture of the system consist of blocks that follow the procedural steps given below for the receiver end:

1) Login with correct Information.
2) Generate the OTP and Select a file which you want to downlode from the cloud.
3) Fetch the file from the Location where it is Hide.
4) The original file will be stored in Hashmap and on cloud the file will be searched which is the Encrypted File.
5) On Encrypted File the Two-fish and AES algo is applied and File will be Decrypted File.
6) Enter correct key to download file
   - if key is correct then allow access to download othewise denied access to download.
7) Apply correct AES key on Encrypted File
   - if key is correct then Decrypt and allow access to file o/w denied accessibility.

B. PROPOSED RESULT

The main objective of this proposed work is to use algorithms like AES, Quantum key generation and two-fish for Encryption, Decryption and Downloading. The security of the system will be enhanced by this combination and hence effiency of the system will be improved.

- **Input**

  User Authentication, GPS Location, Files, OTP, E-mail.

- **Operation**

  Encryption, Authentication, Security, Decryption, IP Restriction over the network.

DOI: 10.15680/IJIRCCE.2016. 0409114

- **Output**

Output will be a verified and the file which is decrypted it will be reliable to download.

IV. CONCLUSION

In this system we propose to have Maximum Security provided to the user data stored or uploaded on cloud network. Secured file Authentication with hybrid of AES algorithm embedding the concept of key management entitled quantum key distribution and Two Fish algorithm for Encryption and Decryption has potential impact not only Authentication but also on files over the cloud. User Authentication can be done by TOTP a time based onetime-password algorithm. We have also provide IP restriction over the Network i.e. Fixed IP address OTP at time of login and downloading, Encrypted Email, Log is maintained. We have also maintained a file access user log, Data leakage and a Security alarm to a user to specify more data Security.

REFERENCES

1. Nikhil Gajra, Shamsuddin S Khan, Pradnya Rane,' Private cloud Security: Secured User Authentication by using Enhanced Hybrid Algorithm', International conference on advances in communication and computing technologies(IEEE), Volume 5, Issue 8, pp. 80-87, August 2014.
2. Rajan.S.Jamgekar, Geeta Shantanu Joshi ,'File Encryption and Decryption Using Secure RSA', International Journal Of Emerging Science and Engineering (IJESE) ISSN: 2319–6378, Volume-1, Issue-4, pp 11-14, February 2013.
3. Cong Wang, Qian Wang, and Kui Ren, Wenjing Lou,'Ensuring Data Storage Security in Cloud Computing', proceedings of 17 th International workshop on Quality of service,IWQOS,IEEE Xplore, pp 1-9,2009.
4. Slawomir Grzonkowski and Peter M. Corcoran Grzonkowski, S., & Corcoran, P. M. ,'Sharing cloud services: user authentication for Social enhancement of home networking'.IEEE Transactions on Consumer Electronics,Volume 57(3), 1424-1432, August 2011.
5. Patel Megha, Prof.Arvind Meniya ,'Prevent DDOS Attack Using Intrusion Detection System in Cloud', International Journal of Computer Application ,Volume 2 ISSN: 2250-1797, Issue 3,pp 905-104,April 2013.
6. SherinJobe, VenifaMini.G and JeyaA.Celin J.,'Efficient RFID Authentication in Cloud Computing', International Journal of Science, Engineering and Technology Research (IJSETR), Volume 2, Issue 4, and pp 954-957, April 2013.
7. Jadapalli Nandini, Ramireddy Navateja Reddy,'Implementation of Hybrid Cloud Approach for Secure Authorized Deduplication', International Research Journal of Engineering and Technology (IRJET) Volume: 02 Issue: 03 | e-ISSN 2395-0056 p-ISSN: 2395-0072, pp 1297-1306, june 2015.
8. Volker Fusenig and Ayush Sharma,'Security Architecture for Cloud Networking', International conference on computing networking and communication year 978-1-4673-0009-4/12/$26.00 (IEEE) and pp 45-48,2012.
9. Nimi P Baby, Dr Salaja Silas,'Study on Privacy and Security Methodologies in Cloud Storage', International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 1, ISSN: 2277 128X,pp 943-946, January 2014 .
10. Ranjana Badre ,'Cloud storage with improved access control and assured deletion', International Journal of Innovations in Engineering and Technology (IJIET) , Volume 3 ISSN: 2319 – 1058, Issue 3 , pp 92-97, February 2014.
11. Prassanna.J, Punitha.K, Neelanarayanan.V,' Towards an analysis of data accountability and auditing for secure cloud data storage', 2ndInternational Symposium on Big Data and Cloud Computing (ISBCC'15) Procedia Computer Science 50,Volume 50, pp543 – 550, 2015.
12. N. Mahesh kumar ,'Auditing Services in Cloud Computing For Achieving Data Access Control', IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 1, Ver. VII PP 52-54,feb 2014.
13. Sunita Rani, Ambrish Gangal ,'Cloud Security with Encryption using Hybrid Algorithm and Secured Endpoints',Sunita Rani et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (3) ISSN:0975-9646, pp 4302 – 4304,2012.
14. http://www.tutorialspoint.com/cloud_computing/cloud_computing_public_cloud_model.htm.