International Journal of Engineering and Techniques - Volume 4 Issue 2, Mar – Apr 2018

RESEARCH ARTICLE OPEN ACCESS

# Data Security in Cloud Environment Through Data Logs

[1]Prof. Sachin Darekar, [2]Akshada J. Dherange, [3]Kshitija B. Kadam,[4]Pranjali B. Nikam.

[1,2,3,4]BharatiVidyapeeth College Of Engineering.Sector-7,C.B.D,Belpada,Navi Mumbai-400614, India

## Abstract:

This Paper proposes use of public cloud for storing and accessing confidential data. Data confidentiality is assured by using encryption technique, in which the data is stored on public cloud is encrypted using encryption algorithm. The encryption algorithm used in encryption technique is AES.With the help of this method of using public cloud, the cost efficiency increases as public clouds provide many services such as service on demand, scalability, pay per use, inexpensive hardware set-up etc. There is a vulnerability to data security while using public cloud, since for confidentiality one has to rely on third party, but if encryption technique is used with data logging to keep track of the people accessing the cloud then the vulnerability to the data confidentiality can be eliminated.

*Keywords* — **SAAS, PAAS, IAAS, Encryption, Accountability, Logging, Cloud service provider.**

## I. INTRODUCTION

In current era, cloud computing is a model of information exchange, which is often outsourced to be stored at a third party, such as cloud providers. However, there have been wide privacy concerns that the information/data could be exposed to those third party servers and to unauthorized parties. Due to this security is a major concern in cloud computing.[1]

The use of cloud computing is increasingly popular due to the potential cost savings from outsourcing data to the cloud service provider (CSP). One technique to protect the data from a possible untrustworthy CSP is that the data owner to encrypt the outsourced data.

In the era of Google Drive and Dropbox, gone are the days when companies would use hard drives, religiously, for storage purposes. Cloud computing has replaced the archaic, storage tools of yesteryears with the easy to use and accessible anywhere, cloud.

In a **SaaS** (Software as service) you are provided access to application services installed at a server. You don't have to worry about installation, maintenance or coding of that software. You can access and operate the software with just your browser. You don't have to download or install any kind of setup or OS, the software is just available for you to access and operate. The software maintenance or setup or help will be provided by SaaS providers and you will only have to pay for your usage.

**IaaS** (Infrastructure as service) provides the infrastructure such as virtual machines and other resources like virtual machine disk image library, block and file-based storage, firewalls, load balancers, IP addresses, virtual local area networks etc. **Infrastructure as service** or **IaaS** is the basic layer in cloud computing model.

## II. LITERATURE SURVEY

| Srno | Name of paper | Author and publication | Technology used | Advantages |
|---|---|---|---|---|
| 1. | ABE for Fine-grained Data Access Control: | Cong Wanget al., [Cong Wanget al., 2010] | Attribute-Based Encryption (ABE),a generalization of identity-based encryption. Attribute-Based Encryption (ABE) not only offers fine-grained access control but also prevents against collusion. | 1.Encrypt file and store. 2.Scalability |

| | | | | |
|---|---|---|---|---|
| 2 | An Efficient. Certificate less Encryption for Secure Data Sharing in cloud | Seung-Hyun, Mohamed Nabeel, Xiaoyu Ding, and Elisa | Cryptography technique specifically public key infrastructure with dynamic password. This paper uses trusted third party establishment of the necessary trust level and provides ideal solutions to preserve the confidentiality, integrity. | 1 Partial decryption attacks are not possible. 2. Hybrid encryption is considered a highly secure |

In ABE there are some disadvantages such as the encryption technique is poor and it has revocation problem as the private keys given should be updated whenever a user is revoked. These issues are overcome by the proposed system.

In Efficient certificate less Encryption for secure data sharing in cloud has disadvantage: key escrow problem. This is also resolved in the proposed system.

## III.Architectural Diagram of Proposed System

In this paper, we propose a framework and a set of mechanisms for storing data in cloud and data access control to store in semi-trusted servers like cloud. To store data in cloud, foreasily achieving fine-grained data and for scalable data access control we leverage AES Algorithmtechniques to encrypt each data file and store in cloud.

In order to protect the data stored on a semi-trusted server, we adopt AES as the main encryption primitive. Using AES, access policies are expressed based on the users or data which enables to

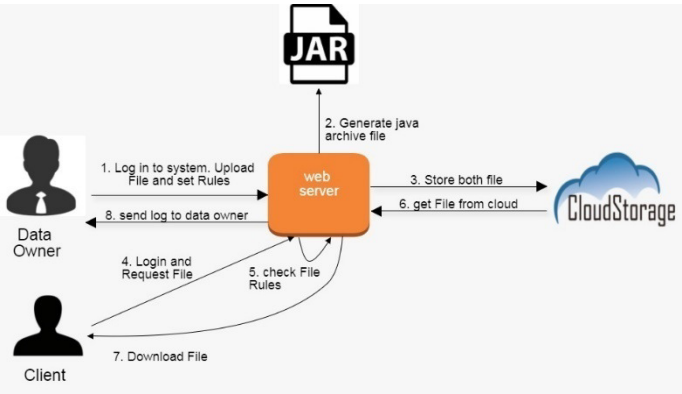



**Fig1. Architecture Diagram**

selectively share bank data among a set of users by encrypting the file, without need to know a complete list of users.

Proposed system is where each client executes an encryption engine that manages encryption operations on data file when file is stored into the cloud. Once the user logins, the cloud service provider verifies if the user is a privileged user or not. After verification the user requests for the data. The request is logged by the cloud service provider. Then the user receives the decrypted data and downloads the data at the client side.

In case of any unauthorized access an error message is triggered and logging details are forwarded to the dataowner.

### *AES Algorithm*

The Advanced Encryption Standard (AES) is a symmetric key block cipher algorithm. The AES has three fixed 128-bit block ciphers with cryptographic key sizes of 128, 192 and 256 bits. Key size is unlimited, whereas the block size maximum is 256 bits. The AES design is based on a substitution-permutation network (SPN) and does not use the Data Encryption Standard (DES) Feistel network.

1. Key Expansions—round keys are derived from the cipher key using AES key schedule. AES requires a separate 128-bit round key block for each round plus one more.
2. Initial Round
   a.Add Round Key—each byte of the state is combined with a block of the round key using bitwise XOR.
3. Rounds

a. Sub Bytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.

b. Shift Rows—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.

c. Mix Columns—a mixing operation which operates on the columns of the state, combining the bytes in each column.

d. add RoundKey

4. Final Round (no Mix Columns)

a .Sub Bytes

b. Shift Rows

c.AddRoundKey

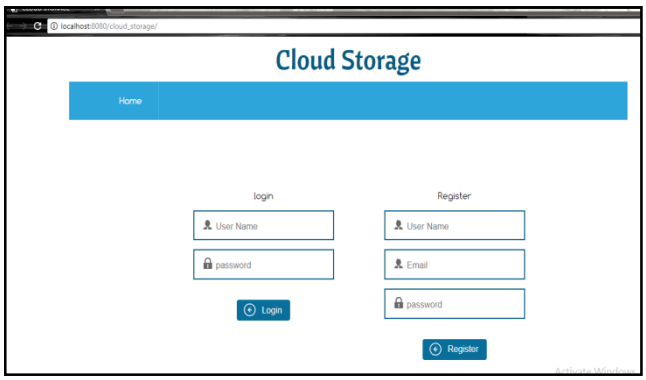
In the proposed system the application lets the client himself/herself to encrypt the data before uploading the data to the cloud.

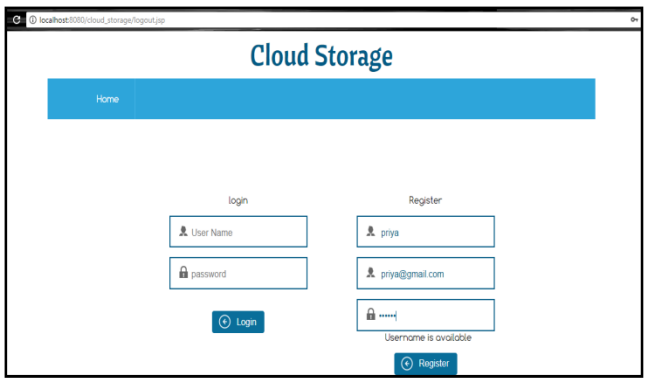
Clients of the system first have to register themselves to the application. Then the clients / users of the application can login to the system whenever required using the login feature as shown in figure 2.

Clients/users of the system can upload files using file upload feature of the system. Clients / users can view files, download files, view requests, requests for files uploaded by other users using various features present in

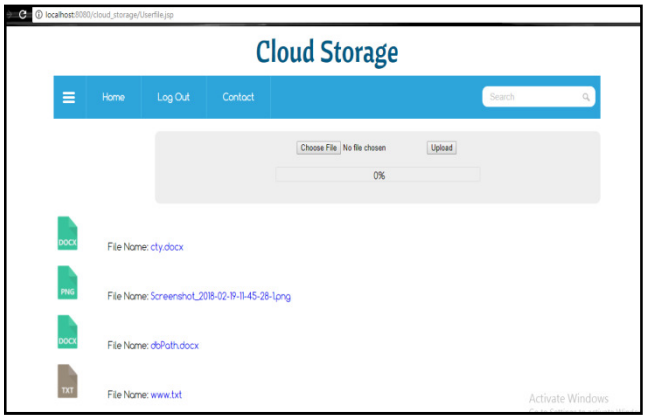
the proposed system.

**Screenshots:**






## IV. Conclusion

We propose a new method in managing access control based on encryption technique and role based access control. Our technique does not depend on cloud to ensure data security. We ensure the confidentiality by encrypting data before uploading whereas access control can be assessed by using access policies. Accountability of data is maintained by generating data logs for additional security purpose.

## Reference


1. *"Cloud Computing Security" Wikipedia , http://en.wikipedia.org/wiki/Cloud_computing_security*
2. *PriyaKharmate, Prof RanjeetsinghSuryawanshi, "Cloud based two tier security scheme for store,share and audit our data into cloud."*
3. *Victor Chang,MuthuRamachandran,Member,IEEE, "Towards achieving data security with the cloud computing adoption framework."*
4. *Sura Khalil Abd, Azizol B HJ Abdullah, Salman Yussof, "Cloud Computing Security Risks with Authorization Access for secure Multi-Tenancy Based on AAAS Protocol."*
5. *IEEE PAPER –Data security : The challenges of cloud computing Hu Shuijing University shanghai of political science and law, Shanghai, china 2001701 , 2014*
6. *S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proc. of IEEE INFOCOM, 2010.*