Digital Sign Enabled Secure Scalable Private Cloud for Data Storage: A Survey

Ajay Gaware, Omkar Parthe, Ajay Mahamuni, Omkar Patil

(Student, Dept. of Information Technology ZCOER Pune, Maharashtra, India)

Assistant Prof. Umesh Nanavare

(Assistant Professor, Department of Information Technology, ZCOER, Pune, Maharashtra, India)

***Abstract** – Cloud Computing is now a worldwide concept which is being utilized by majority of internet users. The number of institutions, companies and other personal users relying on the resources provided by the cloud and as well storing the critical information in the cloud has increased drastically over the years due to the simplistic and attractive features it possesses. One of the main challenging issues that needs to be tackled in the cloud computing is the security of data stored in the service providers' site. When storing data on cloud, one might want to make sure if the data is correctly stored and can be retrieved later. As the amount of data stored by the cloud for a client can be enormous, it is impractical OR might also be very costly to retrieve all the data, just to make sure that it is stored correctly.*

Hence there is a need to provide such guarantees to a client. Hence, it is very important for both the cloud provider and the user to have mutual trust such that the cloud provider can be assured that the user is not some malicious hacker and the user can be assured of data consistency, data storage and the instance he/she is running is not malicious. In this paper, thorough study and analysis is done on some of the research papers that has been written and published in this field. This paper presents literature survey on variety of approaches for implementing data security in cloud computing. The proposed system gives the concept of digital signature to maintain the trust worthiness.

I. INTRODUCTION

With Any client/small organization/enterprise that processes data in the cloud is subjected to an inherent level of risk because outsourced services bypass the "physical, logical and personnel controls" of the user. When storing data in the cloud, one might want to make sure if the data is correctly stored and can be retrieved later. Hence there is a need to provide such guarantees to a client. Hence, it is very important for both the cloud provider and the user to have mutual trust such that the cloud provider can be assured that the user is not some malicious hacker and the user can be assured of data consistency, data storage and the instance he/she is running is not malicious.

Many organizations use the traditional system for data storage. They use the database as backend storage. The organization data is available in huge amount. So there is a major issue in data storage capacity. To overcome this problem the many organization uses the cloud for the data storage.

CSP provides a different scheme for data storage. The data owner can save the file in the cloud. If someone request for any file from the cloud storage, then it can get direct access to that file. They do not provide any access control for file access and file storage to any user.

Cloud Service Provider (CSP) provides different resources and services to the user anytime anywhere over the internet. Due to this feature of cloud maintain security over the cloud is complex. Cloud computing security issues are authentication of the user, nonrepudiation, authority, confidentiality, privacy, availability, access control and checking the integrity of data. Here we have proposed the secure architecture for the cloud which is going to map some cloud security issues that are authentication of the user, confidentiality, privacy, access control and checking the integrity of data. For authentication of the user, the system uses One Time Password (OTP), for data integrity check system uses modified SHA-2 hash function. This modified version of SHA-2 will provide a better solution for Pre Image attack and Collision attack and for encryption and decryption system uses standard Advanced Encryption Standards.

II. RELATED WORK

There are many benefits of using cloud computing such as cost efficiency, quick deployment, improved accessibility etc. However, there are yet many practical problems which have to be solved. The data confidentiality is one of them. Many researchers contributed their efforts to minimize the data security issue in this domain with different solutions that described in this work. A literature review of the works in the area of cloud computing data security is conducted and the results of review are presented in this paper. The results show that the majority of approaches are based on encryption (45%) out of which 71% encryption techniques results are validated. 67% of encryption techniques used experimentation to validate the results. These results point towards the fact that most of researchers show their interest in encryption technique to enhance the security of data in cloud computing environment. The results also reveals the fact of lack of validation in proposed approaches as 42% of the studies provide no validation of the results out of which 67% are guidelines. Only few studies have used statistical analysis for validation. This area (validation) needs the attention of the research community to gain the trust and confidence of cloud computing users.

Cloud Service Provider (CSP) provides different resources and services to the user anytime anywhere over the internet. Due to this feature of cloud maintain security over the cloud is complex. Cloud computing security issues are authentication of the user, nonrepudiation, authority, confidentiality, privacy, availability, access control and checking the integrity of data. Here we have proposed the secure architecture for the cloud which is going to map some cloud security issues that are authentication of the user, confidentiality, privacy, access control and checking the integrity of data. For authentication of the user, the system uses One Time Password (OTP), for data integrity check system uses modified SHA-2 hash function. This modified version of SHA-2 will provide a better solution for Pre Image attack and Collision attack and for encryption and decryption system uses standard Advanced Encryption Standards.

III. LITERATURE SURVEY

The paper [1] solves the problem of limited storage space in the private cloud by using de-duplication technique. The paper gives an incorporate de-duplication for different categories of files.

Deduplication is a well-known optimization technique used in backup storage that divides the file into several chunks. The workload for the cloud storage was categorized and suitable chunking and hashing techniques were identified to reduce the computation overhead. The SHA-1 (64 bit) algorithm is used to find the hash values of these chunks.

The proposed system [2] focus on data protection for cloud storage including following points, 1) Cryptographic Key 2) cryptographic key can be revoked efficiently by integrating the proxy re-encryption and key separation techniques and 3) The data is protected in a fine-grained way by adopting the attribute-based encryption technique. In this paper the fine-grained two-factor data protection method is used for cloud storage which can separate the secret key into two parts, one can be stored in a potential-insecure place, and the other is stored in a tamper-resistant device. Only if one of them is kept secret, the system remains secure.

Combines the cloud-side access control and data owner-side CP-ABE based access control,[3] to solve the security problems in privacy-preserving cloud storage. This technique can also prevent the EDoS attacks by providing the cloud server with the ability to check whether the user is authorized in CP-ABE based scheme, without leaking other information. In CP-ABE, each user has some attributes and data owners encrypt their files with an access policy over attributes. Users in the system hold their own secret keys associated with their attribute sets. If and only if the user satisfies the access policy, the user can decrypt. Communication Overhead can also be reduced in the system.

The integrity and confidentiality of the data uploaded by the user is ensured doubly by not only encrypting it but also providing access to the data only on successful authentication. The existed file on the device will be encrypted using the AES algorithm. To enhance security; AES key will be encrypted using RSA algorithm and will be stored in intern server.[4]

FASTEN is an FPGA-based secure system for processing big data is explained in [5]. It provides the security features in modern FPGAs such as crypto engines and PUF. In FASTEN, the kernel functions for data processing are translated into hardware using a High-Level Synthesis and are executed inside the FPGA fabric. The client's data are stored in encrypted form all the time in CSP, and the actual data processing takes place inside programmable logic. Experimental results show that the FASTEN provides both performance and security advantages over the system with Hadoop's native security support, at the expense of additional hardware.

The proposed system protects data privacy, allows fine-grained access control, enables dynamic user management, supports data provider anonymity and traceability and provides secure data provenance by using

ciphertext-policy attribute-based encryption(CP-ABE)[6].

The data privacy-preserving issues are analyzed by identifying unique privacy requirements and presenting a supportable solution that eliminates the possible threats towards data privacy. The proposed system also gives the privacy-preserving model (PPM) [7] to audit all the stakeholders in order to provide a relatively secure cloud computing environment. The paper provides a methodology to audit a TPA for minimizing any potential insider threats. In addition, CUs can use the proposed model to periodically audit the CSPs using the TPA to ensure the integrity of the outsourced data. The result of the proposed system helps to identify the effectiveness, operational efficiency, and reliability of the CSPs. In addition, the results demonstrate the successful rate of handling the negative role of the TPA and determining the TPA's malicious insider detection capabilities.

A cryptographic scheme for cloud storage, based on an original usage of ID-Based Cryptography is explained in [8]. The system is based on a specific usage of IBC. First, the cloud storage clients are assigned the IBC–PKG function. So, they can issue their own public elements and can keep confidential their resulting IBC secret. Second, a per data key which is derived from a data identifier is used to encipher data. Provides secrecy for encrypted data which are stored in public server. The system offers controlled data access and sharing among users so that unauthorized users or untrusted servers cannot access or search over data without client's authorization.

D. Hodanić et al.[9] gives a hybrid cloud solution. A private cloud is hosted on a public cloud infrastructure, making a tradeoff between security and privacy on one side and cost on the other. It allows even benefit small to medium businesses with very limited resources to leverage benefits of the private cloud solutions.

The paper [10] describes security issues on data isolation, intra-cloud data migration and inter-cloud data migration under the environment of a Private Storage Cloud (PSC) extended with a Partner/Public Cloud. The security solutions based on the HDFS layer, with master/slave architecture, for the PSC are proposed. And an implementation of these security services is given with AOP method. The performance analysis of them proves the efficiency of the security design. Security policies based on HDFS for PSC are implemented:

1) a flexible access control policy based on RBAC (Role-Based Access Control) and CW (Chinese-Wall);

2) a label-based intra-cloud data replicating and restructuring policy

3) a temporary-ticket based parallel inter-cloud data transmission policy.

A digital envelope scheme [11] is used to store and share documents in a private multi-cloud storage gives privacy, integrity and reliability guarantees.It also allows us to share documents with a fine-grained access control, it also allows us to preserve the integrity of the information through digital signatures and to add new information through a secure annotations structure that enables users to have a dynamic interaction.

Main ideas: the encryption of the main information by using cryptographic systems, the construction of a document-sharing envelope by using attribute-based encryption and digital signature mechanisms, and the development of a well-defined assurance workflow to transport the information through the different security phases.

IV. PROPOSED SYSTEM

It is very important for both the cloud provider and the user to have mutual trust such that the cloud provider can be assured that the user is not some malicious hacker and the user can be assured of data consistency, data storage and the instance he/she is running is not malicious. The proposed system gives the concept of digital signature to maintain the trustworthiness.

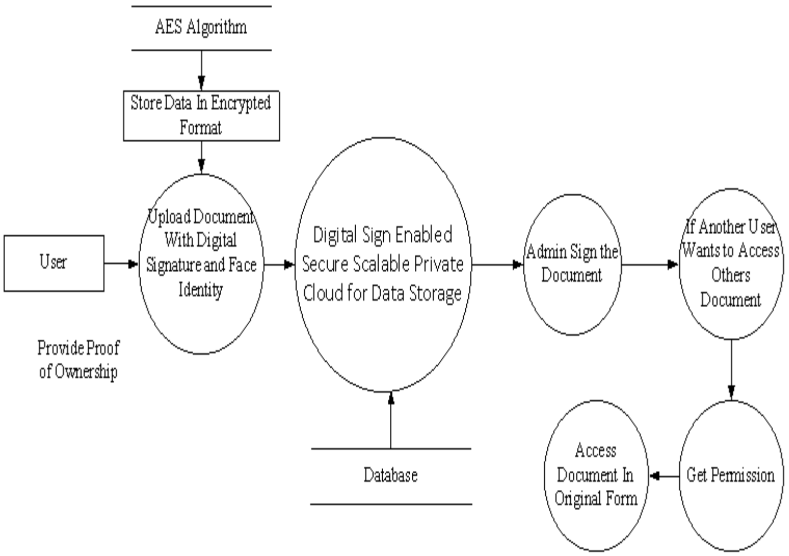
AES Algorithm
Store Data In Encrypted Format
User
Upload Document With Digital Signature and Face Identity
Provide Proof of Ownership
Digital Sign Enabled Secure Scalable Private Cloud for Data Storage
Database
Admin Sign the Document
If Another User Wants to Access Others Document
Get Permission
Access Document In Original Form

Figure: - Flow of the Proposed System

Following are the key components of the proposed system;

- **STEP 1 - Proof of Ownership→** Data Owner uploads document, metadata on a cloud after encryption from Data Owner and Cloud Service Provider. Also, each and every document has a digital e-signing. And all text documents should be able to be modified by authorized users.

- **STEP 2 - Proof of Authentication→** Each user has a one unique username and after signing in to the system authorized user gets OTP on register mobile number for authentication. Each user has a unique digital e-sign because they are used for upload documents.

- **STEP 3 -File Upload With Digital Signature→** Prior uploading the document, digitally sign every individual document. Digital signatures can provide the added assurances of evidence to origin, identity and status of an electronic document, transaction or message, as well as acknowledging informed consent by the signer. So we use digital signatures for File Upload.

- **STEP 4- Upload File & Grant permissions→** Suppose Data owner upload documents with Encryption format and using digital signature. If XYZ user want to access this document which is upload by authorized person that time XYZ user will sent the request to authorized person then authorized person can give permission to XYZ user. with its permissions, because now a day security is very important. Permissions are Read, Write and Append.

- **STEP 5 - Share File→** Document owner can share data with other users which are use private cloud. Provide different types of permissions to users.

- **STEP 6 - Store File in Encrypted Format →** Encryption is the process of transforming information in such a way that an unauthorized third party cannot read it, a trusted person can decrypt data and access it in its original form though. There are a lot of popular encryption/decryption methods, but the key to security is not a proprietary algorithm. The most important thing is keeping the encryption key (password) a secret so only trusted parties know it. Encrypt everything to protect your data so each file will be stored in Encrypted Format.

V. ALGORITHM

1. AES Algorithm

a. Encryption

You take the following AES steps of encryption for a 128-bit block:

1. Derive the set of round keys from the cipher key.
2. Initialize the state array with the block data (plaintext).
3. Add the initial round key to the starting state array.
4. Perform nine rounds of state manipulation.
5. Perform the tenth and final round of state manipulation.
6. Copy the final state array out as the encrypted data (cipher text).

Each round of the encryption process requires a series of steps to alter the state array.

These steps involve four types of operations called:

1. Sub-Bytes
2. Shift-Rows
3. Mix-Columns
4. Xor-Round Key

b. Decryption

As you might expect, decryption involves reversing all the steps taken in encryption using inverse functions:

1. InvSub-Bytes
2. InvShift-Rows
3. InvMix-Columns

Operation in decryption is:

1. Perform initial decryption round:
    - Xor-Round Key
    - InvShift-Rows
    - InvSub-Bytes
2. Perform nine full decryption rounds:

    Xor-Round Key

    InvMix-Columns

    InvShift-Rows

    InvSub-Bytes
3. Perform final Xor-Round Key

VI. CONCLUSION

Data Security in Cloud Computing is an important area that should be given much attention. There we discussed the various systems that gives secure Cloud computing services. Based on the information presented in this study, through the analysis of various papers and the insight from the implementation of the proposed techniques, it is realized that majority of the papers give much attention to data confidentiality, Integrity, Availability and Non- repudiation. By surveying the techniques given by the researcher we come to know that none of the system can guarantees that the data is stored correctly.

So there is need to develop a system that can give the high security and authorized access to the cloud data.

VII. REFERENCES

[1] B.Prabavathy; P. Ramya; ChitraBabu, “Optimized private cloud storage for heterogeneous files in an university Scenario”, International Conference on Recent Trends in Information Technology (ICRTIT) Year: 2013.

[2] Cong Zuo, Jun Shao, Joseph K. Liu, Guiyi Wei and Yun Ling"Fine-Grained Two-Factor Protection Mechanism for Data Sharing in Cloud Storage",IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY,2017.

[3] Kaiping Xue, Senior Member, IEEE, Weikeng Chen, Wei Li, Jianan Hong, Peilin Hong ,"Combining Data Owner-side and Cloud-side Access Control for Encrypted Cloud Storage",information: DOI 10.1109/TIFS.2018.2809679, IEEE Transactions on Information Forensics and Security.

[4] Zaid Kartit, Mohamed EL Marraki, “Applying Encryption Algorithm to Enhance Data Security in Cloud Storage”, Advances in Ubiquitous Networking, Lecture Notes in Electrical Engineering, vol 366. Springer, Singapore, Year: 2015.

[5] Boeui Hong, Han-Yee Kim, Minsu Kim, Lei Xu, Weidong Shi, and Taeweon Suh"FASTEN: An FPGA-based Secure System for Big Data Processing",IEEE DESIGN & TEST HARDWARE ACCELERATORS FOR DATA CENTERS,2017.

[6] Hui CUI,Robert H. DEN G,Yingjiu LI,"Attribute-based cloud storage with secureprovenance over encrypted data",018 February, Volume 26, Issue 4, Pages 461-472

[7] Nesrine Kaaniche, Aymen Boudguiga, Maryline Laurent"ID based cryptography for secure cloud data storage".

[8] Zaid KartitEmail authorAli AzougagheH. Kamal IdrissiM. El MarrakiM. HedabouM. BelkasmiA. Kartit"Applying Encryption Algorithm for Data Security in Cloud Storage",he International Symposium on Ubiquitous Networking, Lecture Notes in Electrical Engineering 366.

[9] D. Hodanić; N. Vrkić; M. Tomić “Data storage and synchronization in private cloud”, 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) Year: 2015.

[10] QingniShen; Yahui Yang; Zhonghai Wu; Xin Yang; Lizhe Zhang; Xi Yu,” SAPSC: Security Architecture of Private Storage Cloud Based on HDFS” 26th International Conference on Advanced Information Networking and Applications Workshops Year: 2012.

[11] Jedidiah Yanez-Sierra; Arturo Diaz-Perez; Victor Sosa-Sosa; J. L. Gonzalez, “A digital envelope scheme for document sharing in a private cloud storage ”, 12th International Conference & Expo on Emerging Technologies for a Smarter World (CEWIT) Year: 2015.