RESEARCH ARTICLE OPEN

Security and Privacy through Multiple Clouds in Cloud Computing

[1]arputha Nilasini.A, [2]anli Sherine.S.M
[1]arputha.nilasini@gmail.com, [2]anlisherine@gmail.com
[1]M.E, Final year, CSE, [2]Assistant Professor, CSE
Loyola Institute of Technology and Science, Thovalai

Abstract
While considering the security and privacy of cloud one can't ignore different threats to user's data on cloud storage. Simultaneous usage of multiple clouds are effective way to ensure the data security in the cloud. The proposed system implements the concept of multiple cloud architecture along with encryption, decryption and de- duplication techniques. Rather than storing complete file on single cloud system. It will split the file in different clouds then encrypt and store them it on different clouds.

I. INTRODUCTION:

Cloud Computing is the latest technology that is used by many organizations and many cloud providers have been arise. Many organizations came forward to establish cloud providers for the users. The users have to trust the cloud provider to secure his data.

Cloud providers should address privacy and security issues as a matter of high and urgent priority. In different clouds the security can be achieved by more than one cloud server. The possibility of entering a malicious insider into the cloud will be reduced.

This is because the cloud provider from which the user is accessing his data is difficult to be known to the unauthorized users. The privacy issues for security will be achieved through the various authentication techniques maintained by different cloud providers in the unrelated cloud environment.

When user is interacting with many clouds which are from different sub cloud providers of different cloud servers then the security level will be increased.

Cloud computing architecture refers to the components and subcomponents required for cloud computing. These components typically consist of a front end platform, back end platforms, a cloud based delivery, and a network. Combined, these components make up cloud computing architecture.

Cloud computing architectures consist of front-end platforms called clients or cloud clients. These clients comprise servers, fat clients, thin clients, zero clients, tablets and mobile devices.

These client platforms interact with the cloud data storage via an application, via a web browser, or through a virtual session.

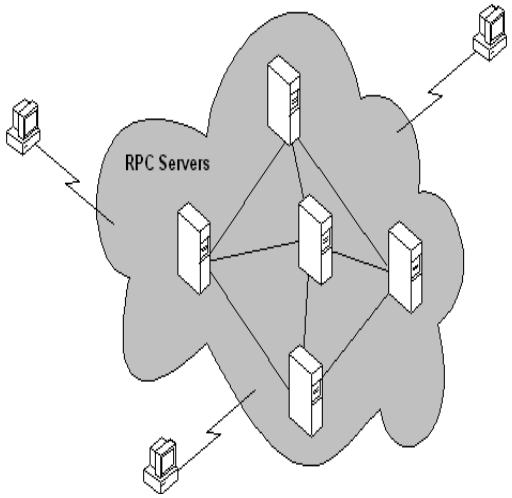

Figure 1: Architecture of Computing

The zero or ultra-thin client initializes the network to gather required configuration files that then tell it where its OS binaries are stored. The entire zero client device runs via the network. This creates a single point of failure, in that, if the network goes down, the device is rendered useless.

A online network storage where data is stored and accessible to multiple clients. Cloud storage is generally deployed in the following configurations: public cloud, private cloud, community cloud, or some combination of the three also known as hybrid cloud. In order to be effective, the cloud storage needs to be agile, flexible, scalable, multi-tenancy, and secure.

The software-as-a-service service-model involves the cloud provider installing and

maintaining software in the cloud and users running the software from their cloud clients over the Internet. The user's client machines require no installation of any application-specific software - cloud applications run on the server. SaaS is scalable, and system administration may load the applications on several servers.

Platform as a service is cloud computing service which provides the users with application platforms and databases as a service. This is equivalent to middleware in the traditional delivery of application platforms and databases.

Infrastructure as a service is taking the physical hardware and going completely virtual. This is the equivalent to infrastructure and hardware in the traditional method running in the cloud. In other words, businesses pay a fee to run virtual servers, networks, storage from the cloud. This will mitigate the need for a data center, heating, cooling, and maintaining hardware at the local level.

1.1. Cloud Components:

Cloud Computing is "a model for enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services).

There are five characteristics, three delivery models and four deployment models in cloud environment architecture. The five characteristics are On-demand self-service, Location independent resource pooling, Broad network access, Rapid Elasticity and Measured service.

The three delivery models are infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). The deployment models are public, private, hybrid and community models.

- **Single Cloud**

In single cloud environment, a third party authentication is used where the information is encrypted and stored in the server. The decryption techniques are known to the user. But it is a failure model because the hacker can easily decrypt the text and steal the information of the user.

- **Multi Clouds**

In multi clouds the security levels are enhanced and the solutions for security risks like data integrity, data intrusion and service availability have been answered. But if the hacker knows the cloud provider that the user is accessing his data then he can easily hack the data.

So the existing techniques in the multi clouds provide the security upto a certain level but not completely. This model which consists of cloud of clouds can solve the security problems by using the secret sharing algorithm.

II. MODULES

- **Directory creation**
- **Cryptographic encryption**
- **De-duplication**
- **Multiparty computation**
- **Cryptographic decryption**

2.1 DIRECTORY CREATION

While creating a new user two directory will create, one directory in cloud one and one directory in cloud two. Then two primary key will generate for those two directories. Each and every user have a different key information.

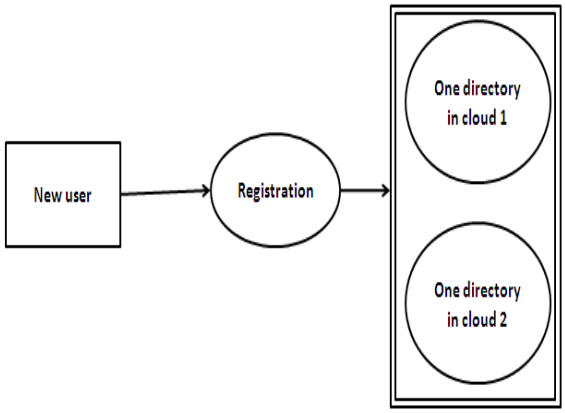

Figure 2: Directory creation

Distribution enhances the performance, manageability, and availability of a wide variety of applications and helps reduce the total cost of ownership for storing large amounts of data.

Partitioning allows tables, indexes, and index-organized tables to be subdivided into smaller pieces, enabling these database objects to be managed and accessed at a finer level of granularity.

Oracle provides a rich variety of partitioning strategies and extensions to address every business requirement. Moreover, since it is entirely transparent, partitioning can be applied to almost any application without the need for potentially expensive and time consuming application changes.

2.2 CRYPTOGRAPHIC ENCRYPTION

Probably, the most basic cryptographic method to store data securely is to store the data in encrypted form. While the cryptographic key could remain at the user's premises, to increase flexibility in cloud data processing or to enable multiuser systems it is beneficial to have the key available online when needed.

This approach, therefore, distributes key material and encrypted data into different clouds. For

instance, with XML data, this can be done inside the XML document by using XML encryption.

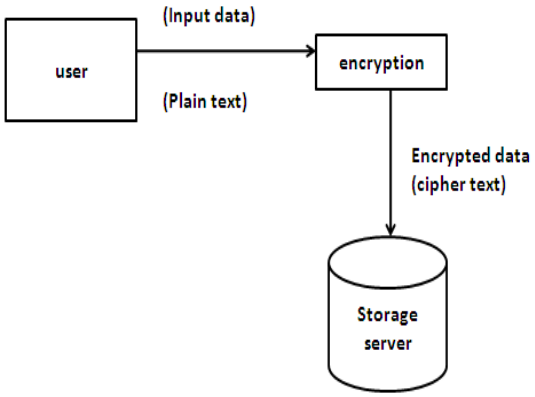

Figure 3: Cryptographic encryption

A similar approach is taken by several solutions for secure Cloud storage: The first approach to cryptographic cloud storage is a solution for encrypted key/value storage in the cloud while maintaining the ability to easily access the data.

It involves searchable encryption, as the key component to achieve this. Searchable encryption allows keyword search on encrypted data if an authorized token for the keyword is provided. The keys are stored in a trusted private cloud whereas the data resides in the untrusted public cloud.

This approach appears to be the most viable alternative, both from the technical and economical point of view. State-of-the-art encryption of data with adequate key management is one of the most effective means to safeguard privacy and confidentiality when outsourcing data to a cloud service provider.

Encryption is considered as an important technical security measure however, some additional mandatory legal safeguards still apply. For personally identifiable data, this means that, e.g., adequate contracts for the export of data to countries outside of the European Economic Area have to be in place.

2.3 DEDUPLICATION

Data de-duplication is a technique for reducing the amount of storage space an organization needs to save its data. In most organizations, the storage systems contain duplicate copies of many pieces of data. For example, the same file may be saved in several different places by different users, or two or more files that aren't identical may still include much of the same data.

De-duplication eliminates these extra copies by saving just one copy of the data and replacing the other copies with pointers that lead back to the original copy.

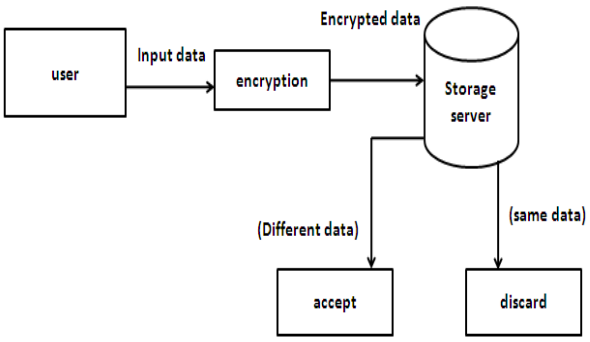

Figure 4: De-duplication

In its simplest form, de-duplication takes place on the file level; that is, it eliminates duplicate copies of the same file. This kind of de-duplication is sometimes called file-level de-duplication or single instance storage (SIS). De-duplication can also take place on the block level, eliminating duplicated blocks of data that occur in non-identical files.

Block-level de-duplication frees up more space than SIS, and a particular type known as variable block or variable length de-duplication has become very popular. Often the phrase "data de-duplication" is used as a synonym for block-level or variable length de-duplication.

2.4 MULTIPARTY COMPUTATION

The idea of secure multiparty computation was first presented in as a solution to the millionaires problem: Two millionaires want to find out who is richer without disclosing any further information about their wealth.

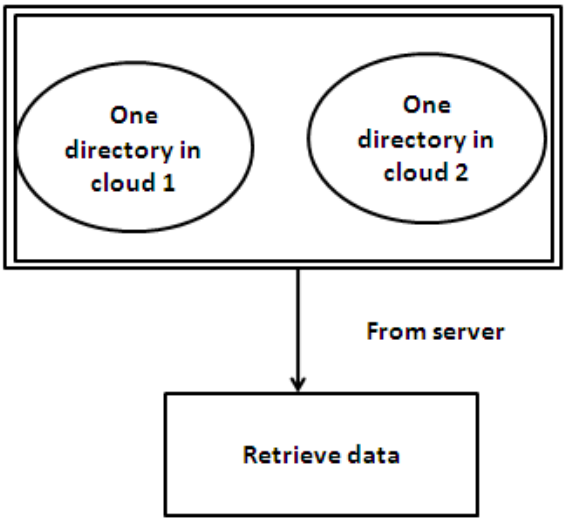

Figure 5: Multiparty Computation

Two main variants of secure multiparty computation are known: Based on linear secret

sharing or garbled circuits. Schemes based on a linear secret sharing scheme work as follows: The user computes and distributes the shares to the different clouds.

The clouds will jointly compute the function of interest on these shares, communicating with each other when necessary. In the end, the clouds hold shares of the result which is sent back to the user who can reconstruct the result.

At least three clouds are necessary for this scheme and no two of them should collude. The approach of garbled circuits works as follows: One cloud generates a circuit that is able to compute the desired function and encrypts this circuit producing a garbled circuit, which is however still executable.

Then, this cloud assists the users in encrypting their inputs accordingly. Another cloud needs now to be present to evaluate the circuit with the user's inputs. Thus, this scheme requires in general only two clouds.

2.5 CRYPTOGRAPHIC DECRYPTION

Decryption is generally the reverse process of encryption. It is the process of decoding the data which has been encrypted into a secret format. An authorized user can only decrypt data because decryption requires a secret key or password.

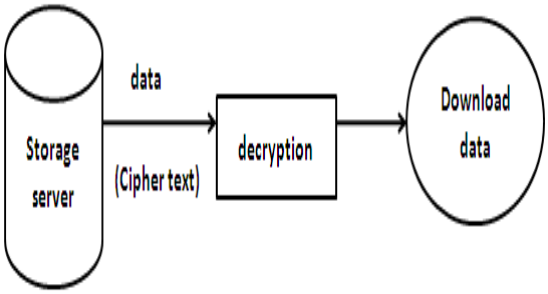

Figure 6: Cryptographic decryption

Decryption is the process of decoding encrypted information so that is can be accessed again by authorized users. To make the data confidential, data is encrypted using a particular algorithm and a secret key.

After encryption process, plain text gets converted into cipher text. To decrypt the cipher text, similar algorithm is used and at the end the original data is obtained again.

III. RESEARCH METHODOLOGY:

There are different architectural patterns for distributing resources to multiple cloud providers. This model is used to discuss the security benefits and also to classify existing approaches. In proposed model system distinguish the following four architectural patterns.

3.1 Replication of Applications allows to receive multiple results from one operation performed in distinct clouds and to compare them within the own premise. This enables the user to get evidence on the integrity of the result.

3.2 Partition of Application System into Tiers allows separating the logic from the data. This gives additional protection against data leakage due to flaws in the application logic.

3.3 Partition of Application Logic into Fragments allows distributing the application logic to distinct clouds. This has two benefits. First, no cloud provider learns the complete application logic. Second, no cloud provider learns the overall calculated result of the application. Thus, this leads to data and application confidentiality. Each of the introduced architectural patterns provides individual security merits, which map to different application scenarios and their security needs . Obviously, the patterns can be combined resulting in combined security merits, but also in higher deployment and runtime effort. The following sections present the four patterns in more detail and investigate their merits and flaws with respect to the stated security requirements under the assumption of one or more compromised cloud systems.

IV. PROPOSED WORK

In proposed system we are implementing the concept of multiple cloud storage along with enhanced security using encryption techniques. We are splits the file in different chunks then encrypt and store it on different cloud. Meta data required for decrypting and rearranging a file will be stored in metadata management server.

- Setting up and configuring different cloud server in order to having storage cloud access. Using cloud server API develop file accessing method in different cloud.
- Developing encryption techniques like AES, RSA for file decryption before storing it on cloud.
- Develop a file management classes. Develop a web interface to upload and download files in cloud storage.

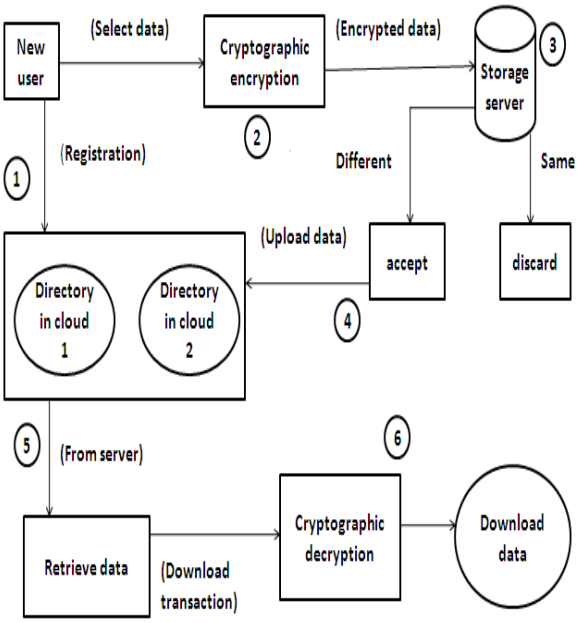

Figure 7: system architecture

The figure shows the architecture diagram of proposed system. **Block diagram** is a diagram of a system in which the principal parts or functions are represented by blocks connected by lines that show the relationships of the blocks.

They are heavily used in the engineering world in hardware design, electronic design, software design, and process flow diagrams. The block diagram is typically used for a higher level, less detailed description aimed more at understanding the overall concepts and less at understanding the details of implementation.

A user interface is the system by which people interact with a machine. The user interface includes hardware and software components. The user distribute data to the server. Each and every user have a different key information.

In cryptography, encryption is the process of encoding messages in such a way that third parties cannot read it, but only authorized party can. Then the secret information will be stored into the multi clouds.

Different clouds are working simultaneously. Every cloud server have different types of data. After the transaction uploaded the data will be retrieved. Then the decryption process will be done. Decryption is the process of decoding data that has been encrypted into a secret format. Finally the transaction will be downloaded.

V. ALGORITHM

5.1 DISTRIBUTED ALGORITHM

A **distributed algorithm** is an algorithm designed to run on computer hardware constructed from interconnected processors. Distributed algorithms are used in many varied application areas of distributed computing, such as telecommunications, scientific computing, distributed information processing, and real-time process control.

Distributed algorithms are a sub-type of parallel algorithm, typically executed concurrently with separate parts of the algorithm being run simultaneously on independent processors, and having limited information about what the other parts of the algorithm are doing.

5.2 SECRET SHARING ALGORITHM

Secret sharing (also called secret splitting) refers to methods for distributing a secret amongst a group of participants, each of whom is allocated a share of the secret. The secret can be reconstructed only when a sufficient number, of possibly different types, of shares are combined together; individual shares are of no use on their own.

In one type of secret sharing scheme there is one dealer and n players. The dealer gives a share of the secret to the players, but only when specific conditions are fulfilled will the players be able to reconstruct the secret from their shares.

5.3 HOMOMORPHIC ENCRYPTION

Homomorphic encryption is a form of encryption which allows specific types of computations to be carried out on ciphertext and obtain an encrypted result which decrypted matches the result of operations performed on the plaintext.

This is a desirable feature in modern system architectures. Homomorphic encryption would allow the chaining together of different services without exposing the data to each of those services, for example a chain of different services from different companies could calculate the tax, the currency exchange rate, shipping, on a transaction without exposing the unencrypted data to each of those services.

There are several efficient, partially homomorphic cryptosystems, and a number of fully homomorphic, but less efficient cryptosystems.

5.4 SECURE HASH ALGORITHM

Its generating a unique number for each data. The resulting hash number is compared to an index of existing hash numbers. If the number is already present means , which is not need to be stored again. Otherwise the new number is added to the index.

VI. CONCLUSION

The use of computing resources as a delivered service is an important development in the world. At present Cloud Computing is a promising

paradigm for delivering IT services as computing utilities. People around the world are making use of different cloud services provided by many companies.

Cloud computing is restructuring how IT resources and services to be used and managed, but major problem in cloud implementation is security challenges. By dividing user's data and applying DNA encryption using data hiding, and then storing it on multiple clouds; this model has shown its ability of providing a cloud customer with a more secured storage. The proposed concepts discussed here will help to build strong security architecture in cloud computing. This will also improve customer satisfaction and will attract more investors for industrial as well as future research farms.

References

[1] Mohammed A. AlZain , Eric Pardede , Ben Soh , James A. Thom, "Cloud Computing Security From Single to Multi Clouds, Department of Computer Science and Computer Engineering, La Trobe University, Bundoora 3086, Australia.

[2] S. Jaya Prakash, Dr K.Subramanyam, U.D.S.V. Prasad, "Multi Clouds Model For Service Availability And Security", Department of Computer Science and Engineering, K.L.University, Vaddeswaram.

[3] Kan Yang, XiaohuaJia, " Attributed-based Access Control for Multi-Authority Systems in Cloud Storage," in Proceeding of 2012 32nd IEEE International Conference on Distributed Computing Systems , IEEE ,2011

[4] "Secure Cloud Computing across Multiple Sensitivity Levels", a white paper by Ratheon Trusted Computer Solutions, 12950 Worldgate Drive, Suite 600 Herndon, VA 20170.

[5] "Security in Private Database Clouds", An Oracle White Paper, July 2012.

[6] Sangdo Lee, Hyoungyill Park, Yongtae Shin: "Cloud computing Availability: Multi-clouds for Big data Service", Department of Computing, Soongsil University, 511 Sangdo- Dong, Dongjak-Gu, Seoul, Korea.

[7] C. Selvakumar G. JeevaRathanam M. R. Sumalatha ," PDDS - Improving Cloud Data Storage Security Using Data Partitioning Technique," IEEE,2012

[8] J.M. Bohli, N. Gruschka, M. Jensen, L.L. Iacono, and N. Marnau, "Security and Privacy-Enhancing Multi-cloud Architectures," IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 10, NO. 4, JULY/AUGUST 2013

[9] Kan Yang, Ren, XiaohuaJia, Bo Zhang, and RuitaoXie, "DAC-MACS: Effective Data Access Control for Multi- Authority Cloud Storage Systems," IEEE 2013

[10] P. Mell and T. Grance, "The NIST definition of cloud computing," National Institute of Standards and Technology, Tech. Rep., Sept 2011.

[11] Jing-Jang Hwang and Hung-Kai Chuang, " A Business Model for Cloud Computing Based on a Separate Encryption and Decryption Service," National Science Council of Taiwan Government, IEEE ,2012

[12] Akash Kumar Mandal, Mrs. ArchanaTiwari , " Performance Evaluation of Cryptographic Algorithms: DES and AES," inProceeding of 2012 IEEE Students' Conference on Electrical, Electronics and Computer Science,IEEE 2012

[13] J. D Assistant Professor, Ramkumar P Systems Engineer, Kadhirvelu D," Preserving Privacy through Data Control in a Cloud Computing Architecture using Discretion Algorithm," in Proceeding of Third International Conference on Emerging Trends in Engineering and Technology,IEEE,2010