International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

A Review of Enhanced Technique for Cloud Data Storage Security Using Data Slicing

Roshan M. Kawale[1], Bharti L. Dhote[2]

Department of Computer Engineering, Sinhgad Institute of Technology, Lonavala(M.S), India

Abstract: ***Cloud computing is a model for using a network of remote servers hosted on the Internet to store, manage and process data. It is a model for enabling widespread and convenient, on-demand access to shared computing resources. It focuses on maximizing the profitable of the shared resources. Cloud computing enables multiple users for accessing a single server to retrieve and update their data, no need to purchase a permit for the different application. In cloud computing, data security is a major issue. After uploading the data on the cloud, data owner has no rights to control the data. For securing the data, everyone wants to trust the third party for the mechanism. The paper proposed an algorithm that consists of data that get slices into different parts. Data present in each slice can encrypt by using a different algorithm. Moreover, the encryption key is applied to data before it stored on the cloud. The objective of our proposed scheme is to store data in a safe and secure manner to avoid data attacks. Another objective is reducing the cost and time required for storing the encrypted data on the cloud.***

Keywords: Security; Authentication; Encryption; Decryption; Data attacks; Slicing;

1. Introduction

With the faster development of information technology, the amount of data produced by organizations has grown exponentially, which makes it hard for many organizations to store cost-effectively and manage the data. Cloud computing is a computing environment in which large group of remote servers are the network. It allows the central storage of data and provides online access to computer resources or services. Cloud computing is a novel business model, and it is considered as one of most cost-effective solutions for organizations to improve their IT segment. Cloud computing provides the advantage of reducing the cost through sharing of computing and storage resources. It is an environment that can use for utilizing an on-demand provisioning mechanism and a pay-per-use model. Cloud computing has drawn many attentions in recent years. Cloud computing environments is a network of computers, connected via the internet, which can use for exchanging, sharing the various resources provided by cloud providers satisfying the need like scalability, usability, and resource requirements. The a variety of problems facing in sharing of computing resources, users can easily solve their problems with the resources provided by the cloud. By using cloud computing services, users can store their critical data in servers. Moreover, they can access their data anywhere from the Internet and do not need to worry about system breakdown or disk faults.

Different users present in the system can share their data, information, and work. They can also play the games together present in a single system. Cloud computing services would provide by the different companies such as Microsoft, Amazon, Google, IBM, and Yahoo. In cloud computing environment, we used three types of cloud environment:

- Internal clouds,
- External clouds
- Hybrid clouds

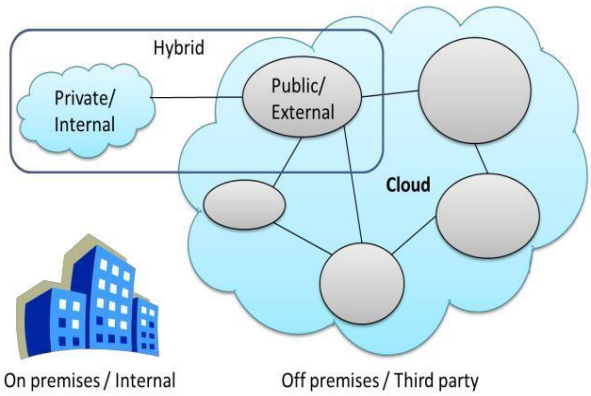

Fig : Cloud Computing Types

Internal clouds: It is call as Private clouds. It is a type of private network that offers various cloud computing services for a limited number of users within the internal network. For example, some companies, universities, and colleges used their internal networks to provide cloud services for their users. This centralized storage of data present in the clouds offers the highest level of security and control. However, they also require that the company need to purchase. Moreover, it maintains all the software and infrastructure, which reduces the cost savings.

External clouds: It is call as public clouds. External clouds can use for the public users, such as enterprises that provide cloud computing services. It deals with the cloud in traditional form, by the internet, and resources that are a dynamical provision on self-service, via the web applications/web services, from a third-party provider who builds on a fine-grained utility computing basis. It is a type of general cloud available to public over The internet.

Hybrid clouds: It is a combination of multiple private and public clouds. To access the various cloud services user should have its identity. Providing security in a private and public would be easy as compared with hybrid cloud because the public or private cloud has only one service provider in the cloud.

There are three widely referenced cloud computing models

are illustrated as follows:

1) **Software as a Service (SaaS)**: It is a type of cloud service which can give to the user by giving user efficiency to access services provided by the cloud computing, running on simple software such as a browser. For example Gmail, Google Groups. It is well-known as ASP or Application Service Provider model.
2) **Platform as a Service (Paas)**: It is a type of service that allows the users to develop applications and deploy them. For Examples, Google App Engine allows developers to create customized apps.
3) **Infrastructure as a Service (IaaS)**: It is a type of service that allocate users to access the servers computational and storage infrastructure in a centralized manner. For example, we have an Amazon Web Services. It allocates remote access to Amazon.com's computing services.

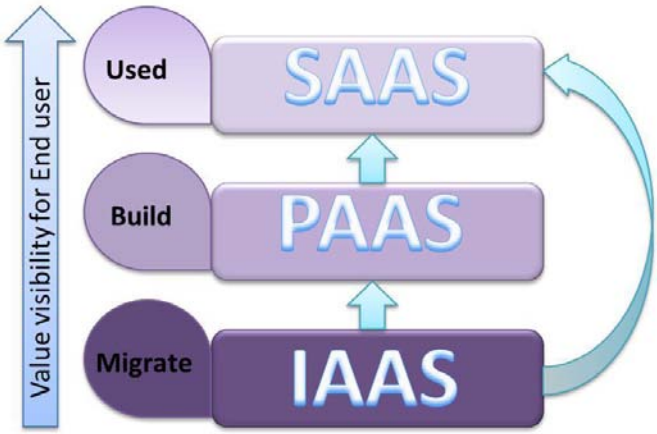

Fig : Services of cloud

The remaining part of paper is divided as follows: Issues in cloud describes in section II. Related work are summarized in section III. The data slicing and cryptography describes in section IV. Finally the paper is concluded in section V.

2. Issues in Cloud

Security is an essential service to would-be provides to the clients; a cloud service provider should assure. Secure cloud is a type of cloud that stores the reliable source of information. For security professionals, it is an important task to protect the cloud who are in charge. Cloud computing can be protected by protecting the data, making sure data is available to the clientele, using Intrusion Detection System on cloud and which is used to monitor any malicious activities. For the purpose of safety, the service provider's must provide a support system for the clients. So that every client must be capable of recovering their data loss in the cloud atmosphere. Hence, the encryption technique must be adopted in a cloud environment by the service provider's to their client for integrity and authentication of data. When it comes to Security, the cloud has to face many difficulties. The service providers must make sure that the client does not face any problem like data loss or data theft. In the cloud, there is also a possibility whereas the malicious user can penetrate the cloud by impersonates a legitimate user. Moreover, thereby infecting the entire cloud, it affects many customers who are sharing the infected cloud. In cloud computing, we discuss many problems that are as follows:

1) **Infected Application:** Vendor should have the complete access to the server for monitoring and maintenance. Moreover, for preventing anyone of the malicious user from uploading any infected application onto the cloud that will severely affect the customer. The applications are available as a service on the cloud. Cloud providers ensure that services to users and secure this application by implementing testing and acceptance procedures for outsourced or packaged application code. It also requires security measures for an application which will site in the production environment.
2) **Authentication:** It is a respondent device or devices like IP spoofing, RIP attacks, ARP poisoning and DNS poisoning that are too common on the Internet. TCP/IP has some "unfixed flaws" such as "trusted machine". The status of machines that are in contact with each other, and tactic assumptions that routing tables present in the routers will not alter. To avoid IP spoofing we required encrypted protocols wherever possible. They can suggest by avoiding ARP poisoning that requires root access to change in ARP tables; using stationary, rather than dynamic ARP tables; or at least make sure to the changes in ARP tables that can log.
3) **Data Verification:** Things like tamper, loss, and theft, on a local machine, in transit, and at rest of the unknown third-party device, or devices, which occur during remote back-ups. Resource isolation ensures the security of data during processing, by isolating the processor cache in the virtual machines, and isolating those type of virtual caches from the Hypervisor cache.
4) ***Availability:*** Cloud providers assure the customers that they will have their regular and conventional data, and it can use for accessing data and applications.
5) ***Data protection:*** To be considered data must protect from one customer who is properly segregate from that of another. Data must be stored securely when "at rest" and it can move securely from one location to another. Cloud providers consist of systems in place from preventing data leaks or access by third parties. Proper division of duties should ensure that auditing or monitoring cannot be defeat, even by privileged users at the cloud provider.

3. Related Work

A survey of different data security issues related to cloud computing provided by Joshi et al. in 2010, [8] This piece of work focuses on how to achieve the security in cloud computing and which are various ways to enhance the secure, can dependable for the cloud environment. By a variety of issues identifies Farzad Sabahi [9], proposed a system that deals with the problem of an ensuring the integrity of data storage in cloud computing with the help of a Third Party Auditor. It can achieve through the public auditing that is carried out on the users data by the Third Party Auditor.

In 2011, Ashish Agarwal et al. [10], This paper talks about security issues concerned with cloud computing. It has revealed many about many serious security threats that

prevail this field. Kui Ren [13], proposed the publicly auditable cloud data storage that is capable of helping the cloud market become fully well-known. This auditing service can facilitate the data owners' to maintain their data effectively that which is present in the cloud storage. The proposed system accounts the user regarding the usage of their data by both the user and the TPA. Services for the legacy users are made available to the user, who may not only access it, but they can also modify the data in the cloud.

The author Prashant Rewagad et al. [2] propose an architecture for providing security in a cloud network. These systems architecture uses the combination of the digital signature algorithm of Diffie-Hellman and AES encryption.

The author Ashutosh Kumar et al.[11] highlights on providing a secure architectural framework for data gathering and sharing. This spectacular work of this project of this work is that the authors have required permission at a different level.

The authors can focus on security but with a view of use hierarchy. M.Venkatesh et al.In 2012, [12] proposes RSASS system for data safety. This scheme uses RSA algorithm for encrypting large files and storing the data. The system can use for storing large databases. However, the use of linear methods in cloud compromise with the data retrieval speed. Hence, this system is high-quality for static data. Farzad Sabahi [9] explains the scope of various enterprises migrating to the cloud. The author explains how migration to the cloud can benefit to the various enterprise. Cloud computing migration involving the consideration of gravity issue of security.

Aderemi A. Atayero [7], proposed an auditing system that is carried out in such a method in which Third Party Auditor can does its job without requiring the copy of user's data. Also the Third Party Auditor which are not capable of deriving the user's data, at the time of performing the auditing task, Third Party Auditors can verify the accuracy of the cloud data on demand from the cloud user, who without retrieves a copy of the whole data or introducing additional online load to the cloud users performs the auditing.

Block tag authentication is made to handle the data from the cloud storage efficiently. For the data that can store in the cloud database, there is a need for inaccessible data integrity check. It assures the cloud users with a sense of security regarding their data. The third party auditing has to be made available in such a way that no additional burden can necessary to the cloud users. A single Third Party Auditor is proficient in handling multiple auditing tasks, which would easily achieve with the bilinear aggregate signature technique. The author Arjun Kumar specifies a method in 2012 [1] that allows the user to store and access the data firmly from the cloud storage. It also guarantees that only authenticated users can access the data neither the cloud storage provider. This method ensures the privacy and security of data that can store in the cloud. A further advantage of this method is that if there is a security breach at the cloud supplier, the user's data will continue to be secure since all data is encrypted. Users need not worry about cloud providers for gaining access to their data illegally.

In 2013, the author Mr. Prashant Rewagad, Ms.Yogita Pawar [2] focused on the idea of security and authentication. His piece of work makes use of a combination of authentication technique and key exchange algorithm, which blends with an encryption algorithm. This combination is referred to as "Three-way mechanism" because it uses all the three protection system of data security, verification, authentication at the same time.

The author S. Kamara and K. Lauter [3][2] in this paper, make use of digital signature and Diffie-Hellman key exchange algorithm that is blended with (AES) Advanced Encryption Standard encryption algorithm to guard the confidentiality of data stored in the cloud. Even if the key transmission can hack, the facility of Diffie-Hellman key exchange renders it is inadequate since key in transit is of no use without a user's private key, which is confined only to the legitimate user.

Author Mohamed Nabeel, Elisa Bertino Fellow in this paper, focused on the utilization of encrypted cloud data with high-level of a user searching experience. Focus on encryption of data using RSA algorithm.[4]

The author Sushmita Ruj, Milos Stojmenovic, Amiya Naya[5]in this paper an approach, based on two layers of encryption, the data owner, can perform a coarse-grained encryption whereas the cloud can perform a fine-graine encryption on top of the owner encrypted data. The author

Xueli Huang and Xiaojiang Du [6] "Efficiently Secure Data Privacy on Hybrid Cloud" This present a privacy-preserving access control scheme for clouds. This paper not only provides fine-grained access control but also authenticates the user who stores information in the cloud. The cloud, however, does not knows the identity of the user who stores information, but only verify the user's credentials. Key distribution is done in a decentralized way. The drawback in the cloud is that the cloud knows the access policy for each record stored in the cloud.

4. Data slicing and cryptography

Data slicing is done using data fragmentation technique horizontal or vertical or mixed fragmentation technique to creates the segments of data. The whole data set gets sliced into three segments either by using vertical, horizontal or mixed fragmentation technique. These slices of segments are encrypted using three different encryption algorithm. Moreover, then upload this chunk of segments to the cloud. On this chunk of segments use encryption & decryption process before a uploading chunk of data on the cloud and after downloading of a chunk of data from the cloud server. Each chunk encrypted with the different cryptographic algorithm.

Encryption is a process in which the readable data is processed and converted into to unreadable cipher text.

Different cryptographic algorithms that are functional to segments the algorithm like AES, DES, 3DES are implemented on individual segments. This entity algorithm works on each segment simultaneously. The plaintext encrypted and converted into cipher text. This various encryption algorithm provides more security than using a single encryption algorithm to encrypt the data.

5. Conclusion

Cloud computing has recently emerged as a paradigm for managing and delivering services over the internet. The rise of this technology is changing the way of IT rapidly, and providing the promise for computation of utilities in a reality. The benefits offered by this technology, the current technologies are not matured enough to realize its full potential. So many challenges are here in this domain Infected Application, Data Protection, Availability, Data Verification, Authentication by this vast literature survey,we can found that data security on the cloud is a very concern issue, and the security of cloud data is the prime responsibility of cloud provider. Different researchers have focused on the fact that user in general has to access large volumes of data from the cloud in a secure manner. However, the complexity of the cryptographic algorithm used, hasn't been given much importance. The complexity of the algorithm directly affects the speed of data access. So, for proficient data security we need a mechanism that provides secure data encryption as well as a secure shield against data theft. So there is need of such optimistic effective work that should focus on cloud security issues. And builds a mechanism for data security in a cloud environment by using an algorithm that will help in efficient and speedy secured data access.

References

[1] Arjun Kumar, Byung-Gook Lee, Hoon-Jae Lee." Secure Storage and Access of Data in Cloud Computing" In ICTC2012.
[2] Mr. Prashant Rewagad, Ms.Yogita Pawar. "Use of Digital Signature with Diffie-Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing.in International Conference on Communication Systems and Network Technologies 2013.
[3] S. Kamara and K. Lauter, "Cryptographic cloud storage," in Proceedings of Financial Cryptography: Workshop on Real-Life Cryptographic Protocols and Standardization 2010, January 2010.
[4] Mohamed Nabeel, Elisa Bertino Fellow.IEEE" Privacy Preserving Delegate Access Control in Public Clouds".January 2012
[5] Sushmita Ruj, Milos Stojmenovic, Amiya Naya "Privacy-Preserving Access Control with Authentication for Securing Data in Clouds".2012
[6] Xueli Huang and Xiaojiang Du "Efficiently Secure Data Privacy on Hybrid Cloud". IEEE ICC 2013 - Communication and Information Systems Security Symposium.
[7] Orner K. Jasim Mohammad, Safia Abbas, EI-Sayed M. EI-Horbaty: "A Comparative Study of Modern Encryption Algorithms based On Cloud Computing Environment" -2013 IEEE.
[8] Joshi, J.B.D., Gail-Joon Ahn. Security and Privacy Challenges in Cloud Computing Environments. In IEEE Security Privacy Magazine, Vol 8, IEEE Computer Society, 2010, p.24-31.
[9] Farzad Sabahi. Cloud Computing Security Threats and Responses. Communication Software and Networks (ICCSN), IEEE 3rd International Conference,2011.
[10] Ashish Agarwal, Aparna Agarwal. The Security Risks Associated with Cloud Computing. In International Journal of Computer Applications in Engineering Sciences [VOL I, SPECIAL ISSUE ON CNS, JULY 2011] [ISSN: 2231-4946].
[11] Ashutosh Kumar Dubey, Animesh Kumar Dubey, Mayank Namdev, Shiv Shakti Shrivastava. "Cloud-User Security Based on RSA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment". In Software Engineering (CONSEG), CSI Sixth International Conference, Sept. 2012
[12] M.Venkatesh, M.R.Sumalatha, Mr.C.SelvaKumar. "Improving Public Auditability, Data Possession in Data Storage Security in Cloud Computing". Recent Trends In Information Technology (ICRTIT), 2012 International The conference, April 2012.