ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

SITES

Smart And Innovative Technologies In Engineering And Sciences

Gyan Ganga College of Technology

Vol. 5, Special Issue 3, November 2016

Various Techniques to Secure Cloud Storage

Mandvi Mamar[1], Dr Neeraj Shukla[2]

Gyan Ganga Collage of Technology in Jabalpur [1, 2]

Abstract: When it comes to cloud data protection methods, no particularly new technique is required. Protecting data in the cloud can be similar to protecting data within a traditional data centre. Authentication and identity, access control, encryption, secure deletion, integrity checking, and data masking are all data protection methods that have applicability in cloud computing. This paper will briefly review few methods and will note anything that is particularly unique to when these are deployed in a cloud.

Keywords: Protecting data, control, encryption, secure deletion, integrity checking, and data

I. INTRODUCTION

Since the last decade the dependency on use of computer has increased tremendously this has attracted the awareness toward data security. Cloud computing is one such technique. Cloud computing is a technology which can imply on various basic applications such as home utility, medical application and other latest computer trends requirement. Application of the data security service can be deploy in the cloud (a network designed for storing data called data centre) and then these services are offered to users always, whenever they want to use.

The cloud hosted services are delivered to users in paper-use, multi-tenancy, scalability, self-operability, on demand and cost effective manner. Cloud computing has become popular because of the above mentioned services offered to users. All the services offered by servers to users are provided by the Cloud Service Provider (CSP) which is working same as the Internet Service Provider (ISP) in the internet computing. The innovative development in virtualization and distributed computing along with high speed network and low cost attracts the focus of users toward internet services. Internet technology is designed with the new concept of services providing to the users without paying for these services and also stored the data on the local memory.

Cloud architecture comprises of the systems architecture of the software systems involved in the delivery of cloud computing, and this involves multiple cloud components communicating with each other over application programming interfaces, usually web services (Elliptic Curve Cryptography for Securing Cloud Computing Applications, 2013).The basic cloud computing architecture for service providing consist of user or client, a third party auditor and cloud server (Figure 1). In the cloud computing architecture, user is the one who uses the services of cloud. It may be a mobile device or stationary device which request for services to the cloud service provider and then on the basis of user ‟s requests third party auditor, provides demanded services to these users offered by the cloud server. In the cloud computing data is stored in data centers from where data is accessed when or wherever it is required. With the data centers virtual servers are connected in which one or more virtual machines (VM) are situated for computation.

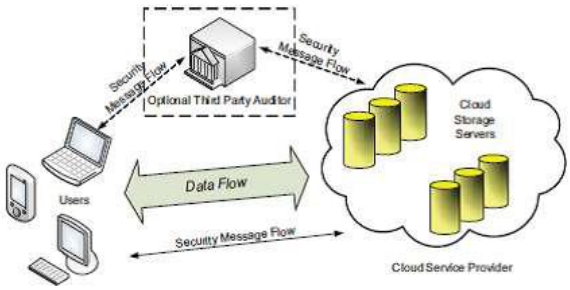

Figure 1: Cloud computing TPA service provisioning architecture [2]

SECURITY SERVICES

To address the concerns outlined above and increase the adoption of cloud storage, we argue for Designing a virtual private storage service based on recently developed cryptographic techniques.

Such a service should aim to achieve the best of both worlds by providing the security of a private cloud and the functionality and cost savings of a public cloud.

Confidentiality: the cloud storage provider does not learn any information about customer data.

Integrity: any unauthorized modification of customer data by the cloud storage provider can be detected by the customer, while retaining the main benefits of a public storage service:

Availability: customer data is accessible from any machine and at all times

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

SITES

Smart And Innovative Technologies In Engineering And Sciences

Gyan Ganga College of Technology

Vol. 5, Special Issue 3, November 2016

Reliability: customer data is reliably backed up.

Efficient retrieval: data retrieval times are comparable to a public cloud storage service.

Data sharing: customers can share their data with trusted parties. An important aspect of a cryptographic storage service is that the security properties described above are achieved based on strong cryptographic guarantees as opposed to legal, physical and access control mechanisms.

SECURITY ISSUES

Security issues that typically occur in cloud data storage have been reviewed by many researchers in the literature.

Most of the attacks to the cloud networks find their root in the traditional network. Some of these have been brought out in this section.

Denial of service: In cloud computing, hacker attack on the server by sending thousands of requests to the server that server is unable to respond to the regular clients in this way server will not work properly.

Counter measure for this attack is to reduce the privileges of the user that connected to a server. This will help to reduce the DOS attack.

Man in the Middle Attack: This type of attack occurs when the secure socket layer (SSL) is not properly installed when two parties are communicating with each other then there is a possibility that all the data communication between two parties could be hacked by the middle party. Therefore countermeasures are required to be taken to protect the data from the middle attack.

Network Sniffing: When the unencrypted data is send on the cloud through the network then the hacker can sniff the passwords from the data on transit.

Port Scanning: There may be some issues regarding port scanning that could be used by an attacker as Port 80(HTTP) is always open that is used for providing the web services to the user.

Other ports such as 21(FTP) etc are not opened all the time it will open when needed therefore ports should be secured by encrypted until and unless the server software is configured properly. Counter measure for this attack is that firewall is used to secure the data from port attacks.

SQL Injection Attack: SQL injection attacks are the attacks where a hackers uses the special characters to return the data for example in SQL scripting the query end up with where clause that may be modified by adding more information in it.

Cross Site Scripting: It is a type of attack in which user enters the correct URL of a website and hacker on the other site redirects the user to its own website and gain access to its credentials. Security threats are usually more common with data protection, browser, and web service .The data stored on the cloud can be easily accessed by the hackers if proper security is not provided to the data. Various methods are elaborated in the literature to overcome these issues some of them are

XML Signature Element Wrappings: It is used to defend a component name, attribute and value from unauthorized party but unable to protect the position in the documents [Jamil D,2011] i.e., the attacker targets the component by operating the SOAP messages and putting anything (malicious modification) that attacker like, so it is difficult for the user to protect his documents.

Browser Security: The browser is expected to make use of SSL (secure socket layer) to encrypt the credentials to authenticate the user prior the data is transmitted over the network. SSL support point to point communication means if there is third party, intermediary host can decrypt the data.

If hacker installs sniffing packages on intermediary host, the attacker may get the credentials of the user and use in these credentials in the cloud system as a valid user [Jensen m,2009].

Data Protection: Data protection in cloud computing is very important factor it could be complicated for the cloud customer to efficiently check the behaviour of the cloud supplier and as a result he is confident that data is handled in a legal way, but it does not like that this problem is intensify in case of various transformation of data. Counter measure for this attack is that a consumer of cloud computing should check data handle and established whether it is handled lawfully or not.

Incomplete Data Deletion: Incomplete data deletion is very risky in cloud computing environment. It does not remove completed data because replicas of data are placed in other servers [Jamil D,2011]. Counter measure is that Virtualized private networks should use for securing the data and used the query that will remove the complete data from the main servers along with its replicas.

LITERATURE SURVEY

A brief review over the techniques which used to provide security in cloud storage is presented in this section. There are various techniques presented by the researchers, which provides an enhanced mechanism for secure storage in cloud. Kadam Prasad, JadhavPoonam, KhupaseGauri, N. C. Thou-tam [1] presents a system to transfer data from data owner to the user in cloud computing.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

SITES

Smart And Innovative Technologies In Engineering And Sciences

Gyan Ganga College of Technology

Vol. 5, Special Issue 3, November 2016

In existing technique there is various type of issue like any unauthorized access provided to the user or data can be leaked during the process of transfer-ring data. Thus in that technique, first user need to provide id and password to login to get authentication to access data then a request to access data is sent to the data owner.
At data owners end data presents in encrypted form, that encryption provides security for the data if data get leaked during the process, a key to decrypt data is provided to the user. By the use of that key user can decrypt data and get access to that data. In that way integrity of the data maintained during the whole process. User does not get access to any other data except that authentication provided to the user because a key is required to access any data.

Nivedita Simbre, Priya Deshpandey [2] presents a TPA and AES encryption based technique to provide security for the data over cloud. In this technique a file distribution mechan-ism is presented in that mechanism a SHA1 is used. When data distributed over cloud in that each block of the file con-tains its own hash code it provides a secure way of sharing of the data.

Further encryption is also required, thus AES encryption is used to encrypt that data. In AES encryption, it is a symmetric key encryption technique which uses single for the encryption and decryption purpose. And TPA is used to pro-vide auditing for that data. In this technique file verifies by comparing it hash values with the backup server's file hash value. This technique quite efficient to provides a secure wayto access data over cloud.

Jian Liu, Kun Huang, Hong Rong [3] a regenerating code based public auditing technique is presented. In this tech-nique, regenerating codes have lower repair bandwidth during fault tolerance. But it only supports public auditing and user need to be present during the whole process of auditing which is practically not possible.

To reduce these short comings an authenticator is designed which uses a proxy for the user in that user generate by using two public key and regenerated by the use of a partial key. In this technique a BLS authenticator is used which uses homographic properties and linear relations among the code blocks, in that way data owner is able to generate authenticator for the new method which quite efficient as compare to the existing technique.

Hemlatha, P Nirupama, V.Balaji [6] a decentralize access control technique is proposed which supports anonymous authentication. In this scheme authenticity of the series is verified and an access control mechanism is used which only allow only authorized user to access the data. And all the operation is perform in decentralized manner not like the other techniques which are centralized.

In this technique there is no un-authenticated users can get access and in this way it can get the privacy preserving in cloud. Madhumita S Patil, Santosh Kumar[7] a TPA based authen-tication technique is proposed in which authentication me-chanism is achieved by the use of Third party auditor, it ensue that data can be accessed by the legitimate user in this mechanism at time of retrieval of the data a mechanism is required in which maintain the authentication otherwise this put huge overhead on user to maintain integrity of the data when more than one user access data simultaneously so third party

Table 1.1: A comparison of the various techniques which used for the secure cloud storage in cloud computing

Technique	Advantages	Disadvantages
Dynamic Secure Auditing Frame-work [9]	Bilinear pairing and Cryptographic techniques are used to provide low computation cost and low communication cost.	In dynamic auditing replay attack and forge attacks can be occurs.
Zero knowledge proof protocol based technique [8]	In this user's personal information is not reveal to the others that preserves integrity of the data.	It not suitable to provide security in public network.
Anonymous Id based technique[5]	provides an scalable data sharing mechanism by using anonymous ID for the operations.	There is no suitable sharing mechanism is provided.
Data coloring and software water-marking technique[4]	A trusted data sharing mechanism in cloud computing is provided.	Inherent defects of watermarking like crop variation, lossy compression are presents in this technique, which generates deformity in the data.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

SITES

Smart And Innovative Technologies In Engineering And Sciences

Gyan Ganga College of Technology

Vol. 5, Special Issue 3, November 2016

CONCLUSION

The way cloud has been dominating the IT market, a major- shift towards the cloud can be expected in the coming years thus data security on the cloud would be the major concern for all the service providers. My survey consists of various existing data storage security techniques for cloud computing.

REFERENCES

[1] KadamPrasad, JadhavPoonam, KhupaseGauri, N. C. Thoutam "Data Sharing Security and Privacy Preservation in Cloud Computing" IEEE, 2015.

[2] NiveditaSimbre, PriyaDeshpandey "Enhancing Distributed Data Storage security for cloud computing using TPA and AES algorithm" IEEE, 2015.

[3] Jian Liu, Kun Huang, Hong Rong, Huimei Wang, and Ming Xian "Privacy Preserving Public Auditing for Re-generating Code Based Cloud storage" IEEE, July 2015.

[4] Kai Hwang, Deyi Li "Trusted cloud computing with secure resource and Data Coloring" IEEE 2010.

[5] L. A. Dunning and R. Kresman, "Privacy Preserving Data Sharing With Anonymous ID Assignment," IEEE Transactions on Information Forensics and Security, vol. 8, no. 2, pp. 402-413, 2013.

[6] Hemlatha, P Nirupama, V.Balaji "Anonymous Authentication for decentralized Access Control of cloud data" IJARCSMS, November 2014.

[7] Madhumita S Patil, Santosh Kumar" Study for En-hancement in privacy preserving authentication protocol using third party in cloud" IJEEM, Vol 3 Issue 1, 2013.

[8] Slawomir Grzonkwoski, Peter M. Corcoran "Sharing cloud service: User Authentication for social Enhancement of Home networking" IEEE Transaction on consumer electronics, Vol. 57, No. 3, August 2011.

[9] Kan yang, XiaohuaJia "An efficient and secure dynamic auditing protocol for data storage in cloud computing" IEEE transactions on parallel and distributed system, Vol. 24 No. 9, September 2013.