Indian Journal of Science and Technology, Vol 9(13), DOI: 10.17485/ijst/2016/v9i13/90588, April 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Survey on Security Issues and Existing Solutions in Cloud Storage

S. Beulah[1] and F. Ramesh Dhanaseelan[2]

[1]Department of Computer Applications, Noorul Islam Centre for Higher Education, Kumaracoil, Kanyakumari – 629180, Tamil Nadu, India; stephenbeulah@rediffmail.com
[2]Department of Computer Applications, St. Xavier's Catholic College of Engineering, Chunkankadai, Nagercoil – 629003, Tamil Nadu, India; fmramesh@yahoo.co

Abstract

Cloud computing is a flexible environment for availing services from cloud through internet on demand. The security issue will reduce the growth of cloud. The data security is a complex problem during adaption of cloud by the users. The existing solutions for the security are considered for analysis. Different types of attacks in the cloud are considered in this survey. Cloud users must understand and vigilant about the risk of data breaches in this environment. A new model required for improving the features of an existing model. The security is a very complex problem in the cloud during the lifetime of the data. The methods for solving this problem is to implement the security as a new service to the users on demand, frequently verify the threats in cloud data and try to resolve it by new methods.

Keywords: Confidentiality, Cloud Security, Cloud Storage, Privacy

1. Introduction

The global market for the cloud will grow to $95million and some percentage of software ill also moved within next five years. This requires the tremendous change in the privacy and security requirements of cloud. This attribute raises many new security challenges[1]. The hackers of cloud storage in the cloud as a honey pot, because of the lack of security and privacy. The main aim of the cloud is to provide better utilization of resources using virtualization[2].

The method of deployment varies depending on the requirements, services and the applications of the stack holder. The organizations maintained the cloud for their own purpose is called Private cloud. The different organizations in the similar interest and requirements are share the cloud infrastructure is called Community cloud. The operation of the community and the private cloud may be in house or by third party. The cloud infrastructure for the public for commercial purpose is called public cloud. The Hybrid cloud infrastructure consists of a number of clouds with different type. But the cloud has the ability to allow data and or application to be moved from one cloud to another by using the interface.

The different stack holders in cloud environment are

- Individuals

There are large numbers of individual users using the cloud services. These users may not have privilege to influence the cloud service directly.

- B. Group

These users may be from same organizations or controlled by same authority.

- C. Service providers

The service providers provide an on demand services like storage, computing or other related services.

2. Cloud Storage and Security

Cloud storage is a model of networked on-line storage where data is stored in virtualized pools of storage which

*Author for correspondence

are generally hosted by third parties. The storage services are provided by storage providers. The storage providers maintain large data centers. People those who require their data to be stored in the cloud may buy or lease storage capacity from them. The virtual resources are utilized by the customers depending on their requirements and the functionality of the resource provider takes care of this in background. The customer's data are stored in the form of files or data objects in the cloud. Physically the resources utilized by the customers are span across multiple servers. The Web-based user interface, Application Programming Interface (API) or cloud storage gateways were used by the customers for their required services. The storage in the cloud is

- A collection of various dispersed resources, but it will act as one.
- Very highly long-lasting through the creation of versioned duplicates.
- Eventually reliable with regard to data replicas

The cost of the cloud storage includes the lease or purchase cost for the required storage size, cost for data transfer, Meta data functions and file deletion functions Storage security is an activity. The implementation of various kinds of safeguards or controls in order to lessen the risk that exploitation or vulnerability in the storage network could cause a major loss to the organization. This view points to the perspective that security is an ongoing process, it is in not a static state, and requires continuing revalidation and modification.

2.1 Information Security

Protecting information and information systems from unauthorized access, disruption, use, disclosure, modification, or destruction to provide our systems and information requires ensuring three things:

- **Confidentiality:** Preventing unauthorized access or disclosure of sensitive information
- **Integrity:** Guarding against destruction of information or improper modification
- **Availability:** Ensuring reliable and timely access information

In addition to the above Access Control and Non Repudiation must be considered in the cloud storage security.

3. Data Storage and its Security

The cloud users are allowed to store huge amount of data into the cloud. The storage service is provided by IaaS. The clients no need to set up data centers for their own, because it requires huge investment. Instead of that, the users use the web services provided by various IaaS providers. The providers charge the users based on the usage of resources. The design goals of cloud storage are storage correctness, dynamic data support, fast localization of data error, authorization, authentication, data availability, data security, etc., the storage service providers take users data and store them in a large data centers and allow the user to access their data anywhere at any time.

The data in the cloud may be lost or modified due to some breaches in the security. The cloud service providers take care of the data resided in their own clod. So t the service providers utilizes the different technologies for the protection of their cloud. But the virtualized nature of the cloud storage needs new technique to handle the security issues in the cloud, the traditional mechanisms are not suitable for handling cloud storage security issues[3]. To secure data in the storage the service providers utilize the existing methodologies such as public and private key encryption. The provider also uses the technique distributed verification of erasure-coded data by utilizing homomorphic token was discussed in[4]. The Remote Data Possession checking (RDPC) schemes are used to verify whether the data is intact or not. An algebraic based RDPC scheme was proposed by[3] to check the data possession in the cloud storage.

The end users utilize the services provided by the cloud and store their data in the provider's infrastructure. The data were not only stored there, but it will be processed by some processor which may be reside anywhere in the cloud. So the security of the data must be considered when the data in different stages. So the following aspects of security must be considered for the different stages of data in the cloud[4].

- Data lineage
- Data during transmission
- Data at rest
- Data in Process
- Data remanence
- Data in source

3.1 Data Lineage

Tracking the data movement in the cloud is referred as data lineage i.e., where it comes in, where it flows to and how it travels through the cloud. This information is important for auditing the cloud. The data lineage solution will record the data sources that are relevant to each stage of the process and then mapping these sources to each other to show how the data flows and how it is transforms. In a public cloud the data lineage problem solving is a challenging task. The data flows non linear in virtual environment. So it complicates the process of data integrity in the cloud.

3.2 Data during Transmission

The data during transmission must be encrypted using the latest encryption technology. The selection of encryption technology must be up to date. The selected technology must provide security against present security threats and by using the protocol the transmission must provide integrity and confidentiality. After encryption the data must be divided into packets and it will be transmitted to the receiver through disjoint paths. It will reduce the chance of capturing all the packets by any threats until the packets are coupled together in a particular format.

3.3 Data at Rest

The data managed even the data in rest during its transmission. Managing this kind of data is feasible in IaaS because of the access restriction over data. The major problem with data at rest is loss in control. Recently the encryption techniques are available with storage devices. The lock box approach, homomorphic encryption and public encryption are some of the techniques to manage the data at rest.

3.4 Data in Process

Data in a cloud will enter into processing state so that the storage cloud requesting the service for processing data in the cloud. Once the process will activate user data available in the storage cloud will securely transferred to the processor for processing. During the processing time the cloud must provide security when the data in process.

3.5 Data Remanence

Data remanence refers to the data will remain in the cloud in case of data transfer or data removal. The data not only be protected against unauthorized access but also securely deleted at the end of its life cycle. Data remanence is also referred as secure delete, secure purging etc., When documents expire, deleted and if a malicious user gets access to the disk or if disk are say physically stolen the chances of extracting the data block is high. So the storage cloud should provide the end users to delete the data securely. Data remanence may be the secure disclosure of sensitive information in an uncontrolled environment. Different techniques have been developed to answer data remanence.

3.6 Data in source

The data must be secure from the source. Data provenance is the security property stating that the source, where a piece of data is generated cannot be spoofed or interferes with. The provenance refers to maintaining data integrity and ensuring that the integrated data are computationally correct.

4. Classification of Security Issues

The security issues for the cloud storage is classified into two categories

4.1 Access Security Issues

Security during communication in the cloud is a potential point at which threats to the service could be exposed. The advent of mobile computing systems a potential threat to security and possibly privacy of users would be a location as this could entail the presence of communication as this to identify the location.

4.2 Service Security Issues

Most of the security threats are possible at the point of service provision. This would include device security and storage security. The providers provide the security by using IDS firewalls and malware protection.

5. Security Issues in Cloud Storage

The issues which were faced during the uses of cloud storage service provided by the cloud closely related with integrity of data, data confidentiality and availability. The different issues are

5.1 Trust the data stored in cloud

Data stored in the cloud must be confidential and consistent after every update process. The integrity of data should also be maintained in the current data. The detection of corrupted service data was very difficult. This may lead to information leakage before being discovered. The Third Party Auditor [5] (TPA) was the agent for the data owners. This TPA has a protocol to do the audit service. Any changes in the outsourced data were monitored by TPA. The TPA raises the periodic verification request by providing optimized schedule.

In [6] authors proposed cooperative PDP scheme to support dynamic scalability on multiple storage servers based on hash index hierarchy and homomorphic verifiable response. The audit performance of PDP scheme, the authors optimizes the probabilistic query and periodic verification.

5.2 Security Lack in Service Provider Agreements

The agreement made by the providers only includes the agreements for high data availability not for the security. For providing better privacy and ensuring data availability, the authors proposed a scheme which can be attained by dividing the user's chunk of data into data pieces. The sharing of data among the accessible SPs in the marketplace efficiently and providing high availability and security by more Secured Cost-effective Multi-cloud Storage (SCMCS) model [7].

5.3 Data History

One of the attribute in local data storage is Meta data. By using this data the user can view the account of data object. For better data integrity verification and roll back facility the history information are used. Currently this feature is available with security vulnerabilities.

5.4 Provable data possession

This issue is related to other issues like the trust on the storage provider, integrity of data etc. The integrity check for the data was performed during data retrieval. It is very difficult to decide how the data was maintained in the storage providers system. The service provider must ensure the data was not leaked to third party. Because the agreement for the service in between the service provider and the customer. The current service providers are care for this issue.

6. Security Threats in Cloud

The main objective of cloud environment is to provide high cloud services, availability, authentication and security. One of the existing survey works classify security threats in cloud based on deployment models [1]. Security of will be considered in three different levels like Network level, Host level and Application level.

6.1 Network Level Security

In current environment the cloud network have different types of communication like shared or unshared, private or public, large area or small area. Each of the above said networks have number of security threats. Security breaches are high in public and large area networks. The security breach needs to be considered are

- Confidentiality and integrity
- Ensuring proper access control
- Trusted encryption scheme and tokenization

Some of the major issues in cloud network are:

- DNS attack
- Reused IP address
- Sniffer attack
- Man in the middle attack
- Denial and distributed denial of Service attack, etc.,

6.2 Application Level Security

The security loopholes in cloud application are:

- Cross site scripting (XSS) attack
- Cookie positioning
- Hidden field manipulation
- SQL Injection attack
- Dictionary attack
- Google hacking attack., etc

Some of the security breaches may be defined below

- **Insecure Storage:** Most web applications uses sensitive information. That information is stored either in a file system or in the database. For example credit card numbers, passwords, and proprietary information or account records, etc., generally sensitive information is protected using encryption techniques. Encryption is generally used to protect user sensible assets.

- **SQL Injection Attack:** In SQL injection attack an attacker tried and modify the SQL statement, then the statement will also executable by the attacker with the same rights as the application user. Various techniques like Avoid constructing SQL queries with user input, avoiding dynamic SQL queries, use procedures instead of queries etc are used to prevent this attack. The authors proposed a new architecture in proxy based system [6] to prevent this attacks. This architecture tries to detect and extract user input for the assumed SQL control sequences dynamically.
- **Cross Site Scripting (XSS) Attacks:** The attacker injects malicious scripts to different users is called Cross-site scripting. The XSS attacks can be categorized into two types: stored and reflected. The injected code was permanently stored in server in the form of message forum or log or in some format and it was injected in the user script. During the execution of data retrieval script in the server the malicious script was executed. In XSS attack the attacker try to block user's session and take over the account. Other damaging problems raised by the intruder is to include the disclosure of end user files, redirecting the user to some other page or site, installation of Trojan horse programs, and modifying presentation of content.
- **Broken Access control:** The user access facilities are controlled by authorization. To ensure proper access control, the web application must verify the authorization checks, and secure authentication. Privileged users from others are distinguished by using this verification.
- **Cross Site Request Forgery (XSRF/CSRF):** Once the user logged into the website this attack compel the user to execute unwanted actions. Another name for this forgery is *hostile linking*. This attack modifies the firewall settings, conduct fraudulent financial transactions and post unauthorized data on a forum. Detecting XSRF is very difficult by the user. The users only know about this attack after the damage has been found in user data and may not be possible to take remedy.
- **Cookie Poisoning:** The unauthorized access of a service in the cloud is done by editing a cookie by cookie positioning attack. The user identity credentials are available in cookies. Once those are accessible the content of cookie may be forged to imitate an unauthorized user. Then this attack will be solved by doing regular cleanup or by using any data hiding technique for cookie data [8].
- **Man in the Middle Attack (MIM):** In this attack the attackers try to intrude the communication between the endpoints on a network. Then the attacker try to inject false information and intercept the data transferred between them. Another name for this attack is Bucket-brigade attack, Monkey-in-the-middle attack etc., The attack usually starts to listen in the process of session, sniffing on a network stream, and ends with trying to alter, reroute or forge the intercepted data.
- **Buffer Overflows (BO):** In this attack the attacker tries to corrupt the execution stack of a web application. Buffer overflow flaws will be present in the web server products or an application server that serve the static and dynamic aspects of the web application.
- **Domain Name Server attacks (DNS):** In this attack the server is called by the user using the server name. But the client has been forwarded to some other spiteful cloud instead of the required cloud by the user. Though using DNS security actions like: Domain Name System Security Extensions (DNSSEC) reduces the effects of DNS threats.
- **Re issue of allotted IP address:** When a particular user moves out of a network then the IP-address associated with the old user is assigned to a new user. This task is more risks due to the security of new user. Because the time lag between the changes of an IP address in DNS and old DNS caches. Here the intruders try to access the old user data by using the IP address in old cache.
- **IP spoofing:** IP spoofing is one of the most common forms of on-line camouflage. In this attack, an attacker gains unauthorized access to a computer or a network newer routers and firewall arrangements can offer protection against IP spoofing.
- **Physical security:** The customers lose control over physical assets in the cloud. So the security model must be reevaluated. For example the biometric hand reader, security cameras must be used to monitor the activity throughout the facility. The heat, air flow, temperature, and humidity should all be kept within optimum ranges for the computer equipments.
- **Dictionary attack:** In this attack the intruder try to more attempts authentication mechanism by entering each word in a dictionary as a password or try to determine the decryption key of an encrypted message or document.

- **Google Hacking:** Google is the best option for searching details regarding anything on the net. By using the Google search engine the attacker try to find sensitive information. That information was used by the attacker for hacking a user's account.
- **Broken Authentication:** The requests submitted by each user are tracked by the session created by the web application. In this attack the attacker hijack the active session by using the session tokens. It is difficult to protect user identity only by protecting authentication credentials, session identifiers in SSL
- **Injection Flaws (Shell Commands and SQL):** This attack allows the attackers to transmit malicious code to another system through a web application. These attacks include the use of external programs.

7. Existing Security Solutions

In[9] focus on the problem of auditing when a un trusted server stores client's data. The authors introduce the model for provable data possession. This scheme minimizes the computation on the server, data block access and the client server communication. This scheme supports spot checking and homomorphic verifiable tags, generic transformation and robust auditing. The tough auditing integrates Remote Data Checking (RDC) with forward Error-correcting codes to moderate arbitrarily small file corruptions and propose a Generic change for adding robustness to any spot checking-based RDC scheme.

Proposed the access control in two different levels[10] that combines coarse grained access control for the cloud. In this scheme communication overhead was acceptable and it limits the information that the cloud learn from partial view of access rules and patterns. It was enforced only at user's side and it handles read and write access control. Proposed a model using an identity based data storage scheme. This model is suitable for inter domain and intra domain queries [11]. The owner can access only one file with the help of one query. This scheme is secure against collusion attacks[12] utilizes the homomorphic encryption. The homomorphic encryption allows the processor to process data without decrypting.

Developed[13] a storage model using disintegration technique, which is based on sensitivity, criticality and value of the data. It provides better security by means of disintegration values of data and also a good technique for prevention of information leaks. The author concludes that the data residing in data center are robbed of their values and that are built up during run time. The newly built data are then destroyed once the usage is completed. So the intruder will not get access to the data. Uses[14] algebraic signature to verify data possession in cloud storage. The author proposed an algebraic based RDPC scheme for improving the efficiency of the verification. This scheme does not use public key technique and it can achieve tens to hundreds of megabytes per second. This mechanism does the verification only comparing the response returned by the storage server. Drawback in this scheme is it lies in its probabilistic security.

The existing problems in RDPC like replay attack and deletion attack were solved here by proposing a new protocol. The proposed protocol utilizing the techniques involving block sequence number and file name during tag generation using pseudo-random functions and the probabilistic auditing was provided by random sampling trick[15]. The SecCloud[16] is a secure computation auditing protocol foe ensuring secure storage and secure computation auditing. This protocol is used to achieve privacy cheating discouragement by batch verification, signature verifier and probabilistic sampling techniques. A capacity based access control model for flexible, secure and scalable cloud storage by D. Harnick et al. This architecture integrates the existing access control solutions and it includes the benefits of capacity based models with other basic mechanisms. An attribute based encryption, proxy re encryption was proposed by[17] for data confidentiality and accountability of user secret key.

Address[11] three services for security in cloud. The services are virtual machine security services, virtual network security services and policy based trust management services[18, 19] uses third party auditor to verify the integrity and dynamic data stored in the cloud. Here the author proposed both audit ability and dynamic data operations. This paper also supports multiple auditing tasks. For introducing multiple auditing the author utilizes the bilinear aggregate signature method. The performance analysis shows this system is highly efficient and provably secure. Addresses[20] a new storage model for cloud environment. During data migration data were split into three types based on the parameter values for Confidentiality, availability and integrity. According to the sensitivity of the data, it was stored into private, public or a limited access area. Then the data were encrypted and stored into the proper places. For fast accessing the index is generated by using index builder for frequently accessed items.

Major drawback in this model is the parameter values and frequent access items were selected and issued by the client or the user. The author uses the digital signature to secure the data with lock and unlock facility. In this model, if the user has the accessibility then the system allow for accessing the data only if the data in unlock ode. If the data is in lock then the access request is in pending[21]. The data stored in the cloud are audited by Third Party Auditor (TPA). Introduce the digital signature for achieving authentication through the TPA[22]. Provides[23] the secure storage and secure data retrieval using public key and master secret key. During data retrieval the end user uses the attribute and cipher text for decryption.

8. Conclusion

Today most of the IT organizations shift towards the cloud, so they can gain best business applications and fast access or drastically boost their infrastructure resources with minimum cost. The main intention for the security for the user data in the cloud is directly proportional to the value of asset it protects. One of the possible solutions for providing security will be with the help of security as a service based on the applications or customer requirements. But the problem in this framework is if the clouds have a common security methodology it will be high value asset. So the hackers target to hack the security service provided by the cloud. In this scenario, the security will be provided as a service in customized method.

Another possible solution for cloud security will be done automatically for the necessary information without expecting any requisition from the customer. This may be achieved with the help of analyzing data exist in the cloud and classify the data which will require security without customer interaction. Any way the cloud attract customers only each and every components of the cloud must be carefully analyzed and an integrated solution must be deployed for better information security otherwise the cloud environment will remain cloudy. My research work concentrated on providing an intelligent security solution to the cloud storage users.

7. References

1. Subhashini S, Kavitha V. A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications. 2011 Jan; 34(1):1–11.
2. Seccombe A, Hutton A, Meisel A, Windel A, Mohammed A, Licciard A, et al. Security guidance for critical areas of focus in cloud computing V2.1. Cloud security Alliances. 2009. p. 1–76.
3. Zhang Q, Cheng L. Cloud Computing: State of the art and research challenges. Journal of internet services and applications. 2010. p. 7–18.
4. Weng C, Wang Q, Ren K, lou W. Ensuring data storage security in Cloud Computing. International workshop of Quality of service. IEEE; 2009. p. 1–9.
5. Zhu Y, Hu H, Ahn GJ, Yau SS. Efficient audit service outsourcing for data integrity in clouds. Journal of Systems and Software. Elsevier; 2012. p. 1083–95.
6. Zhu Y, Hu H, Ahn GJ, Yu M. Cooperative provable data possession for integrity verification in multi cloud storage. IEEE transaction on Parallel and Distributed Systems. 2012; 23(12): 2231–44.
7. Singh Y, Kandah F, Zhang W. A Secured Cost-effective Multi-Cloud Storage in Cloud Computing. IEEE INFOCO, M, Workshop on Cloud Computing. 2011. p. 619–24.
8. Gollmann D. Securing web applications. Information security technical report. Elsevier; 2008; 13(1):1–9.
9. Ateniese G, Burns R, Curtmola R, Herring J, Khan O, Kissner L, Peterson Z, Song D. Remote Data Checking Using Provable Data Possession. ACM Transactions on Information and System Security. 2011 May; 14(1):2.
10. Raykova M, Zhao H, Bellovin SM. Privacy enhanced access control for outsourced data sharing. Financial Cryptography and data security, Lecture notes in Computer Science. 2012. p. 223–38.
11. Hana BJ, Susilo AW, Mua Y. Identity based data storage in cloud computing. Future Generation Computer Systems. 2013. p. 673–81.
12. Maha TEB AA, Hajji S, Abdellatif EL Ghazi. Homomorphic encryption method applied to Cloud Computing. Conference on Network Security and Systems (JNS2) IEEE; 2012. p. 86 – 89.
13. Subashini S, Kavitha V. A Metadata Based Storage Model For Securing Data In Cloud Environment. American Journal of applied Sciences. 2012; 9:1407–14.
14. Chen L. Using Algebraic Signatures to check data possession in cloud storage. Future generation computer Systems. Elsevier; 2012; 29(7):1709–15.
15. Yu Y, Zhang Y, Ni J, Au M H, Chen L, Liu H. Remote data possession checking with enhanced security for cloud storage. Future Generation Computer Systems. Elsevier; 2015 Nov. p. 77–85.
16. Wei L, Zhu H, Cao Z, Dong X, Jia W, Chen Y, Vasilakos AV. Security and privacy for storage and computation in cloud computing. Information Sciences. Elsevier; 2014. p. 371–86.

17. Yu S, Wang C, Ren K, Lou W. Achieving secure, scalable and the fine grained data access control in cloud computing. Proceedings IEEE; 2010. p. 1–9.
18. Wang Q, Wang C, Ren K, Lou W, Li J. Enabling Public auditability and data dynamics for storage security in cloud computing. IEEE Transaction on Parallel and Distributed Systems. 2011; 22(5): 847–59.
19. Wang C, Chow SSM, Wang Q, Ren K, Lou W. Privacy Preserving Public Auditing for Secure Cloud Storage. IEEE Transactions on Computers. 2013; 62(2):362–75.
20. Sood SK. A combined approach to ensure data security in cloud computing. Journal of network and Computer Applications. Elsevier; 2012. p. 181–88.
21. Lee JY. A Study on the Use of Secure Data in Cloud Storage for Collaboration. Indian Journal of Science and Technology. 2015 Mar; 8(S5):33–36.
22. Manjusha R, Ramachandran R. Secure Authentication and Access System for Cloud Computing Auditing Services Using Associated Digital Certificate. Indian Journal of Science and Technology. 2015 Apr; 8(S7); 220–27.
23. Saikeerthana R, Umamakeswari A. Secure Data Storage and Data Retrieval in Cloud Storage using Cipher Policy Attribute based Encryption. Indian Journal of Science and Technology. 2015 May; 8(S9):318–25.