A Review on Contemporary Security Issues of Cloud Computing

Saksham Chandrawat

Master of Science (C.S.)

Pace University, NY, USA

sc35073n@pace.edu

Abstract: Thought the Cloud Computing environment different services allow users to stores the data at remote location. However, there are number of security issue with storing at remote location.This paper shows those issues like Lack of control of data, Lack of Trust and multi-tenancy. Ensuring cloud data integrity is to be the big issue. To overcome this issue Cloud Service Provider use Trusted Third Party Auditor to ensure the integrity. The proposed algorithm handles encrypted data and performs auditing without decrypting data. The algorithm performs auditing over encrypted data.

Index Terms: Cloud Computing, Cloud Security, Integrity, Encryption, Public Auditing.

Introduction

The critical importance of Cloud Computing is increasing exponentially and receiving a growing attention in the scientific and industrial communities. Cloud Computing enables ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be release with minimal management effort or service provider interaction [1].

The main objective is to provide secure, quick, convenient data storage and net computing service, with all computing resources visualized as services and delivered over the Internet [2, 3].The cloud enhances collaboration, agility, scalability, availability, ability to adapt to fluctuations according to demand, accelerate development work, and provides potential for cost reduction through optimized and efficient computing [4-6].

Clients are at the enthusiasm of the cloud specialist organizations for the accessibility and Distributed computing offers client to get to all applications from anyplace on the planet, liberating you from the confines of the desktop and making it simpler for assemble individuals in various areas to work together [10]. Cloud specialist organizations have joined to manufacture cloud conditions and give administrations to the client.

Some of the Challenges of Cloud Computing are as follows:

1. **Data Loss:** Due to outside model of cloud, the client's data may lose its control. The client personality administration is taken care of by the cloud; and the client get to control rules, security strategies, and the cloud supplier oversees requirement. The purchaser needs to depend on the cloud supplier for information security and protection, and accessibility

2. **Information Security**: The Technical Controls are utilized for verify information client and information accessor and get to administration, encryption of information, and other information review taking care of necessities for consenting to administrative prerequisites.

3. **Data Privacy:** Information security tends to the secrecy of informationfor particular elements [13]. Protection covers lawful andobligation concerns. Securing protection in any processing.

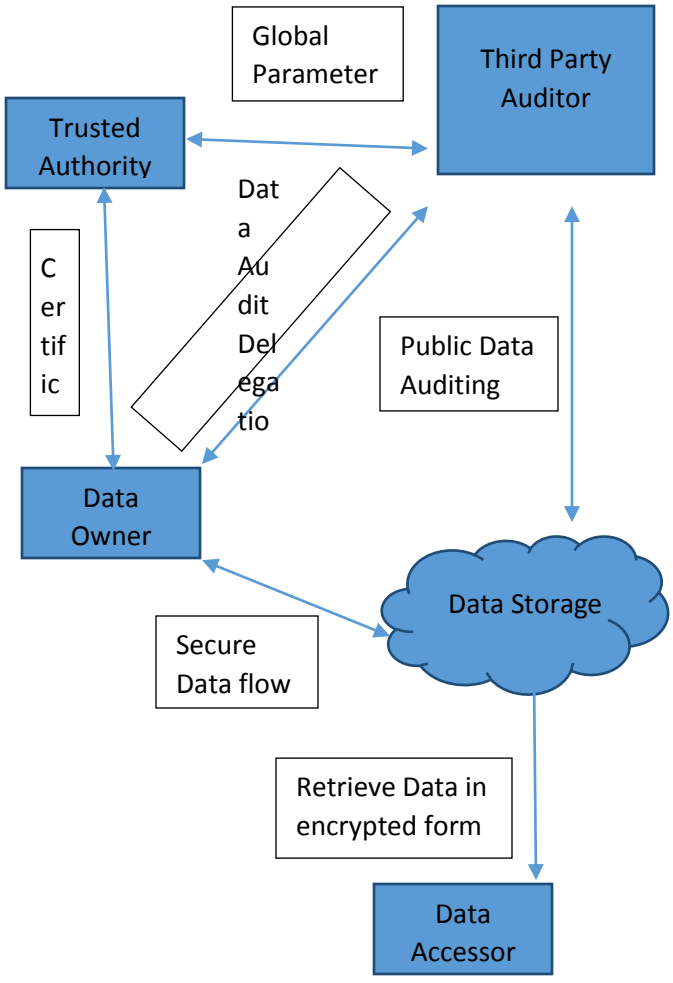
4. **Lack of Trust:** Associations that outsource enter business forms in the cloud may not realize that the contractual workers and might be ignorant of the personality of the sub-contracting cloud suppliers. That is why, 'on-request' and 'pay-as you-go' models might be founded on feeble

confide seeing someone, which include outsiders with proper security.

5. **System Integrity:** The Cloud Security require protection against intentional attacks on its functionality. A cloud consists of stakeholders including consumers, providers and a variety of administrators. It is important to partition the access rights for each of these groups while keeping malicious attacks at bay [8].

Proposed Work

Approach used in proposed system is secure data in cloud storage. The goal of proposed system is to check integrity the data that come under the property of users.Accessor is an individual customer has huge amount of data and necessities to store in cloud. It relies upon the cloud to oversee information and calculation to reduce the capacity cost. Owner uploads data on cloud and send request to provide checking integrity of data.



Public Auditing System Model

Third Party Auditor: A trusted association provide capacities that customer do not have, they are in charge of customer information on distributed storage. Trusted authority provides certificates to data owner for identification purpose.Mashups combine more than one source element into a single integrated unit. Thus, PaaS models also inherit security issues related to mashups such as data and network security .Also, PaaS users have to depend on both the security of web-hosted development tools and third-party services, I am quoting this researcher, see the quotation mark [7].

The procedure flow of open inspecting in a point-by-point way includes the TPA. The information proprietor stores the information in the cloud at first instead of storing the whole; the proprietor isolates the information into various pieces and sends to the remote distributed storage [9]. Proprietor of the data executes key generation algorithm to generate public key and private key. By applying private key data owner encrypts file, it becomes F' and re-encrypt file, it becomes F". Upload double encrypted file and public key to server. To perform audit operation data owner generate audit query, send it to third party auditor along with signature s. Third party auditor generate challenge to server. Server generates proof. Signature from data owner compare with signature of data at server, public key and double encrypted data send by server towards auditor. Using public key auditor decrypts data, compute audit operation. Finally auditor generates result weather data is correct or not. The algorithm runs as data owner to generate public key and private key. It takes λ as input. Outputs a secret key as private key denoted as Pr and public key denoted as Pk. The

Key Generation algorithm is

1: for all i such that i=1 to n do
2: Select two random primes p, q
3: Pr, Private Key
4: Pk, Public Key
5: end for
6: for all i such that i=1 to n do
7: Generate pks, Public Signature Key
8: end for

Algorithm to Encrypt File:here we usedD (data), M (bytes conversion of data), B (Big Integer)H (secure random hashing), G (gcd value), E (encrypted data), S (Signature)

1: Read plain data D
2: Convert data into bytes M
3: Kp= KeyPairGenerator.getInstance("RSA")
{Generate public key ,private key pair Kp}
4: for all i such that i=1 to n do

5: Pk=keypair.getPublic() {Generate public key}
6: Pr=keypair.getPrivate() {Generate private key}
7: end for
8:H=SecureRandom.getInstance("SHA1PRNG,"SUN ") {Calculate Hashing H}
9: r= random.nextBytes(randomBytes)
{Select random bytes r}
10: G=gcd(M) {Calculate gcd value of data}
11: E=((r.modPow(Pk,Pr)).multiply(M)).mod(Pk)
{Encrypt data}
12: S=E.modPow(Pr,Pk) {Generate Signature}

Algorithm to Verify Proof:

1: for all i such that i 1 to n do
2: Calculate R.Sig
3: end for
4: if R.S == S then
5: INTEGRITY SUCCESS
6: else
7: INTEGRITY FAIL
8: end if

The main issue in Cloud storage is data integrity. Public auditing solves the issue and verifies the shared data. Public auditing schemes need to check data privacy, ensure data privacy, provide easy Retrieve ability and prevent from unauthenticated user.As we can identify the vulnerabilities which contribute to executionod the threats and make system more robust. However new security techniques is needed and also to redesigned traditional solutions that can work with cloud architecture.

References

A Review on Contemporary Security Issues of Cloud Computing from IEEE *Xplore* Digital Library

[1] Sookhak, Mehdi, Abdullah Gani, Muhammad Khurram Khan, andRajkumarBuyya. "Dynamic remote data auditing for securing big data storagein cloud computing." *Information Sciences* 380 (2017): 101-116.

[2] Gartner Inc: Gartner identifies the Top 10 strategic technologies for 2011. Online. Available: . Accessed: 15-Jul-2011 *http://www.gartner.com/it/page.jsp?id=1454221* Online. Available: . Accessed: 15-Jul-2011

[3] Zhao G, Liu J, Tang Y, Sun W, Zhang F, Ye X, Tang N: Cloud Computing: A Statistics Aspect of Users. In First International Conference on Cloud Computing (CloudCom), Beijing, China. Heidelberg: Springer Berlin; 2009:347–358.Google Scholar

[4] Zhang S, Zhang S, Chen X, Huo X: Cloud Computing Research and Development Trend. In Second International Conference on Future Networks (ICFN'10), Sanya, Hainan, China. Washington, DC, USA: IEEE Computer Society; 2010:93–97.View ArticleGoogle Scholar

[5] Cloud Security Alliance: Security guidance for critical areas of focus in Cloud Computing V3.0.. 2011. Available: https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf Available:Google Scholar

[6] Marinos A, Briscoe G: Community Cloud Computing. In 1st International Conference on Cloud Computing (CloudCom), Beijing, China. Heidelberg: Springer-Verlag Berlin; 2009.Google Scholar

[7] Xu K, Zhang X, Song M, Song J: Mobile Mashup: Architecture, Challenges and Suggestions. In International Conference on Management and Service Science. MASS'09. Washington, DC, USA: IEEE Computer Society; 2009

[8] Badger, T. Grance, R. Patt-Corner, J. Voas,(2012). Cloud ComputingSynopsis and Recommendations, National Institute of Standards andTechnology

[9] Navajothi, R., and S. Jean Adrien Fenelon. "An efficient, dynamic,privacy preserving public auditing method on untrusted cloud storage." *InInformation Communication and Embedded Systems (ICICES), 2014International Conference on*, pp. 1-6. IEEE, 2014.

[10] Lordemann, David, Daniel Robinson, and Paul Scheibe. "Method andsystem for establishing an audit trail to protect objects distributed over anetwork." *U.S. Patent Application 09/952,696*, filed September 14, 2001.