International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 3, Issue 11, November 2014 **ISSN 2319 - 4847**

Cloud Information Security Using Third Party Auditor and Cryptographic Concepts

Imran Hafiz Sayed[1], Bhagyashree Brijmohansingh Rajput[2]

[1]Student of MCA, MIT College of Engineering, Aurangabad, Maharashtra, India

[2]Student of MCA, MIT College of Engineering, Aurangabad, Maharashtra, India

ABSTRACT

Security for data on cloud is a major issue nowadays. There are certain security concerns and threats which have been defined previously. To overcome some of them we are introducing our research under "Cloud Information Security Using Third Party Auditor and Cryptographic Concepts". In this the Third Party Auditor (TPA) is used to inspect the flow of data in between CSP and Data Owner. The TPA is responsible for protecting the data from the access of an unauthorized user & maintaining the integrity of data. The Data Encryption algorithms are used to store the data on cloud into the encrypted format. The encryption and decryption is performed by the data owner only.

Keywords:- MessageDigest, Encryption, Decryption, Digital Signature.

1. INTRODUCTION

Cloud computing has become hot issue in since 2007 and many companies used to attempt the cloud computing services. Typical cloud computing services are Amazon EC2 and Google's Google app engine, amazons they use the Internet to connect to external users, with the convenience, economy, high scalability and other advantages, Pick up any tech magazine or visit almost any IT website or blog and you'll be sure to see talk about cloud computing as in [22]. Cloud computing gets its name as a metaphor for the Internet. Internet is represented in the network diagrams as a cloud, the cloud icon represents "all that other stuff" that is makes the network work. Cloud computing promises to cut capital costs and operational more importantly, let IT departments focus on strategic projects instead of keeping centralized the data centre running, as in [1].It is up to the clients to decide the vendors, depending on how willing they are to implement secure policies and be subject to 3rd party verifications. Sales force, Amazon and Google are currently providing such services, charging clients using an on-demand policy as in [11] references statistics that suggest one third of breaches due to laptops falling in the wrong hands and about 16% due to stolen items by employees. Storing the data in the cloud can prevent these issues altogether. Moreover, vendors can update application/OS/middleware security patches faster because of higher availability of staff and resources. The Cloud computing change Internet into a new computing platform, is a business model that achieve purchase on-demand and pay-per-use in network, has a broad development expectation as in [22]. The basic point of view pattern is changing the way it is being focused over cloud. In the view of users i.e. In addition to this advantage it brings forth exclusive and challenging security threats towards user's outsourced data.

1.1 Cloud computing security concerns

- Multitenancy [15]
- Information assurance & Data Ownership [14]
- Data Privacy [20]

1.2 Cloud Computing Security Threats

The main 10 security threats of Cloud Computing are mentioned in the table below:-

TABLE 1: THREATS IN CLOUD COMPUTING [21]

Sr. No	Threat	Countermeasures	Layer
1	Data Leakage	Digital Signature FRS Technique Homomorphic	SPI
2	Service or Account Hijacking	Identity and Access Management	SPI
3	Customer Data Manipulation	Web application Scanners	S
4	VM escape	TCCP TVDc HyperSafe	I
5	Malicious VM creation	Mirage	I
6	Insecure VM migration	PALM VNSS	I
7	Sniffing / Spoofing virtual	Virtual network security	I
8	Data Scavenging	Symmetric key Cryptography	SPI
9	Denial of Services	Policies can be offer by cloud providers.	SPI
10	VM Hopping	-	I

1.3 Major Information Security Concerns

Figure 1 Present Information Security Concerns [13]

1.4 Cloud Deployment Models [14]

1.4.1 Public Cloud : It is available publicly - any organization may subscribe

1.4.2 Private Cloud : In this type, services built according to cloud computing principles, but accessible only within a private network.

1.4.3 Hybrid Cloud : It is the combination of Public Cloud and Private Cloud.

1.4.4 Partner Cloud : Here cloud services offered by a provider to a limited and well-defined number of parties.

In this paper, we are focusing only on the users of Private Cloud and Partner Cloud. All the proposed work done below is carried out by taking into the account these two types of users only.

2. METHODOLOGY

The proposed problem is - Integrity of data, Authentication of user and problem of TPA if Third-party-auditor not only uses data but also modify the data than how data owner or user will know about this problem. Here the user has two types' of keys, one of which only the owner knows called private key and another one which is known to anyone called public key. We match both the data it must be same as the sent one on the sender cannot deny that they sent it (non repudiation) [13].It is very important to provide public auditing service for cloud data storage, so that the user trusts an independent third party auditor (TPA). TPA checks the integrity of data on cloud on the behalf of users, and it provides the reasonable way for users to check the validity of data in cloud. Public auditing in addition to user provides the external party to verify the correctness of stored data against external attacks it's hard to find. However these schemes, as in [7] don't involve the privacy protection of the data. It is a main disadvantage which affect the security of the protocols in cloud computing. So users who depend on only TPA for their security storage want their data to be protected from external auditors. I.e. Cloud service provider has significant storage space and computation resource to maintain the users' data. It also has expertise in building and managing distributed cloud storage servers and ability to own and operate live cloud computing systems. Users who put their large data files into cloud storage servers can relieve burden of storage and computation. At the same time, it is important for users to ensure that their data are being stored correctly and security check. Users should be equipped with certain security means so that they can make sure their data is safe. Cloud service provider always online & assumed to have abundant storage capacity and computation power. The third party auditor is invariably online, too. It makes every data access be in control as in [22]. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, storage, or even individual application capabilities, with possible exception of limited user-specific application configuration settings. TPA eliminates the involvement of client through auditing of whether his data stored in cloud are indeed intact, which can important in achieving economies of scale for cloud computing Third Party Auditor (TPA) who will audit the data of data owner or client so that it will let off the burden of management of data of data owner. Released audit report would not only help owners to evaluate the risk of their subscribed cloud data services, but also be beneficial for cloud service provider to improve their cloud based service platform, as in [7].This public auditor will help to data owner that his data is safe in cloud with the use of TPA auditing, management of data will be easy and less burdening to data owner. In cloud computing, security is most important task. Cloud computing entrusts services with users data, software and computation on a published application programming interface over a network. If a smart hacker hacks the cloud server and steals the data and modifies it then in some cases this modification is not even identified by the cloud provider. So, in this case, we take the help of a trusted TPA to check for the integrity of our data. This TPA takes care of our data and makes sure that data integrity is maintained. Our vision for helping assure ongoing system integrity in a virtualized environment includes an evolution of integrity checking competences, as in [5] Each phase, in this evolution relies on secure start up enabled and provides an increasing level of assurance and this evolution begins with one-time integrity checks at system or hypervisor start up as in [22]. The basic proposed architecture of "Cloud Information Security Using Third Party Auditor and Cryptographic Concepts" is as follows:

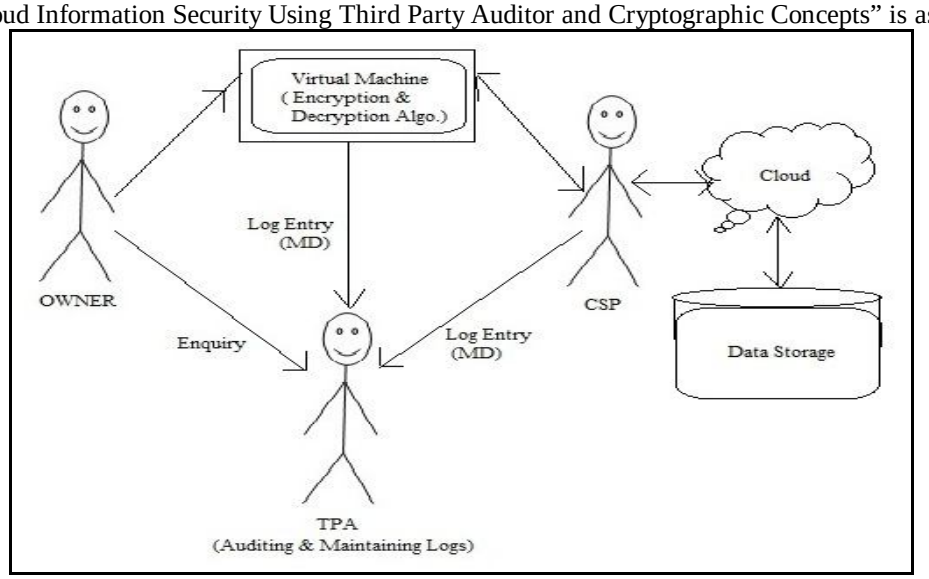

Figure 2 A Basic proposed architecture of "Cloud Information Security Using Third Party Auditor and Cryptographic Concepts".

3. ALGORITHM

1)Owner will send a request message to CSP, the same copy of message will be forwarded to TPA.
2)CSP will check for authentication through login_id & password.
3)If login successful, owner will send a message digest [12], MD(S, FN, A or D).
4)Same copy of MD will be forwarded to TPA.
5)If digital signature [12] S matches.
Then,
CSP will send the data i.e. [MD (FN, F_ID) +F] to the client.
Else
Owner goes back to step-2.
6)Same copy of MD (FN, F_ID) will be forwarded to TPA.
7)Owner will take the file F with F_ID and decrypt [13] it on Virtual Machine and perform desired operation.
8)After completing the task owner will again encrypt [13] the file F to F' on same Virtual Machine.
9)Owner will create another MD (FN, S, M or D or N).
10) After this owner will send the respective MD+F' to CSP and one copy of MD is sent to TPA.
11) Now, If the specified S and F_ID of TPA, CSP and owner matches then,
CSP will perform the specified operation i.e. M, D or N, on F' and a *SUCCESS* message goes to TPA and Owner.
12) If either of S or F_ID doesn't match no updations will be performed and owner goes to step 1 and a *FAILURE* message goes to TPA and Owner.

Where,
S - Digital signature
FN - File Name to be accessed
A - Access the file FN
D - Delete the file FN
M - Modify the existing file
N - Create the New file
F - Requested File
F' - Encrypted F
F_ID - Unique identification number of F on cloud
The Sequence Diagram for the proposed algorithm is shown below:-

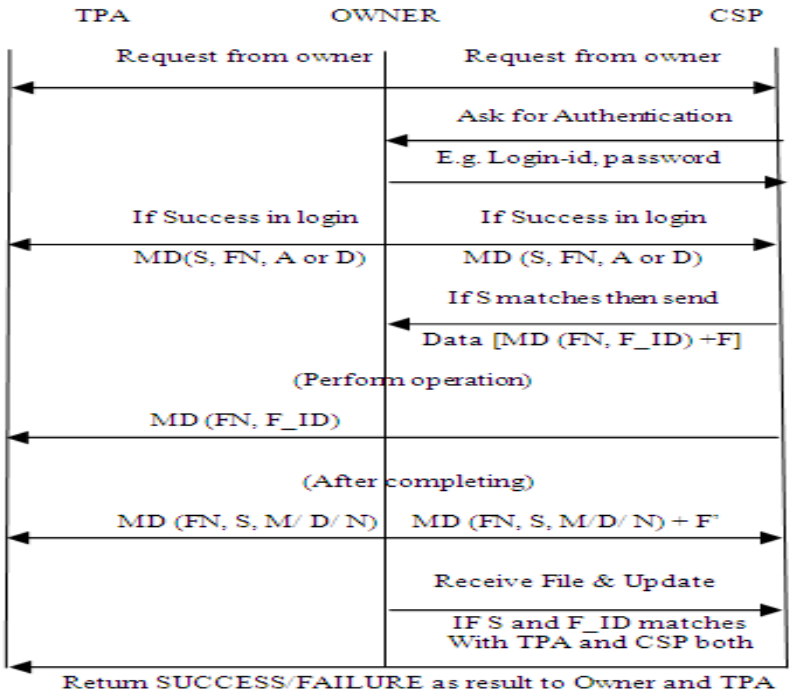

Figure 3 Sequence Diagram for Proposed Algorithm

3.1 Following problems (as stated above in 1.1 and 1.2) can be overcome by using this approach:

1) Multitanancy
2) Information Assurance and Data Ownership
3) Data Privacy
4) Data Leakage
5) Customer data manipulation
6) Data Scavenging

3.2 Threats(Limitations) of proposed work

1) Cost effective
2) Focus is only on Private model users and Partner model users, no security policies are defined here for public or hybrid cloud users.

3.3 Advantage

1) The major advantage of implementing this strategy is that, it has ability to overcome all the Information Security Concerns that are stated above in fig.1 of (1.3).
2) Reduced Data Redundancy because of the provided unique file identification F_ID.

4 Conclusion

Cloud data security is an important aspect for the client while using cloud services. TPA can be used to ensure the security and integrity of data. TPA can be a trusted third party to resolve the conflicts between the cloud service provider and the client. Various schemes are proposed by authors over the years to provide a trusted environment for cloud services. Encryption and Decryption algorithms are used to provide the security to userwhile using TPA. This paper provides an abstract view of different schemes proposed in recent past for cloud data security using TPA. Most of the authors have proposed schemes which rely on encrypting the data using some encryption algorithm and make TPA store a message digest or encrypted copy of the same data that is stored with the service provider. The third party is used to resolve any kind of conflicts between service provider and client.
In this paper we have proposed the scheme in which the TPA will not have any kind of data stored in it. It will just maintain the log of each incoming request and outgoing response through Messege Digests i.e. as its name suggests it will just audit all the transactions happening, and as the data encryption/decryption is done at client side only this scheme also solves the problem of integrity. As TPA also checking the authenticity of owner at any time and client can also check his data at the time of submission which will make this scheme as robust in compare to others.

ACKNOWLEDGEMENT

This work was supported in part by Faculties of MCA department, MIT College of engineering, Aurangabad.

References

[1] Elsenpeter Robert, Anthony T.Velte and Toby J.Velte, Cloud Computing a Practical Approach 2010.
[2] Qian Wang and Cong Wang and KuiRen, Wenjing Lou, Jin Li “Enabling Public Auditability And Data Dynamics For Storage Security in Cloud Computing” in IEEE transactions on parallel and distributed systems, 2011, vol. 22, no. 5.
[3] Cong Wang and KuiRen and Wenjing Lou and Jin Li”Toward Publicly Auditable Secure Cloud Data Storage Services”, in IEEE 2010.
[4] M.Ashah and R. swaminathan and m.baker”Privacy-Preserving Audit and Extraction of Digital Contents” , 2011.
[5] H. Shacham and B. Waters “Compact Proofs of Retrivability“in proc. of asiascrypt, 2008.
[6] Xiang Tan and Bo Ai “The Issue of Cloud Computing Security in High-Speed Railway” international confer. on electronic and mechanical engi. and information technology, 2011. Beijing p.r china,
[7] Farzad Sabahi,“Cloud Computing Security Threats and Responses” ,IEEE confer. 2011, 978-1-61284-486-2/111
[8] Ravi Kant Sahu and AbhishekMohta, L.K. Awasthi ”Robust Data Integration While Using Third Party Auditor For Cloud Data Storage Services”, conf. IJARCSSE, 2012, Volume 2, Issue 2,ISSN: 2277 128X.
[9] Govinda V, and Gurunathaprasad, H Sathshkumar,”Third Party Auditing For Security Data Storage in cloud through digital signature using RSA” IJASATR, 2012, issue 2,vol-4, Issn 2249-9954.
[10] P. Mell and t. Grance “Draft Nist Working Definition of Cloud Computing”, 2009.
[11] Elinor Mills, "Cloud Computing Security Forecast: Clear Skies", 2009.
[12] www.diablotin.com/librairie/networking/puis/ch06_05.htm by S Garfinkel - â€Ž1999

[13] https://cseweb.ucsd.edu/~mihir/cse207/classnotes.html Introduction to Modern Cryptography. By: Mihir Bellare and Phillip Rogaway
[14] Cloud Computing – Benefits, Risks and Recommendations for Information Security, November 09, by European Network and Information Security Agency (ENISA)
[15] en.wikipedia.org/wiki/multitanency
[16] www.ccsenet.org/cis
[17] Arduino http://arduino.cc/en/Guide/HomePage
[18] OpenCV Library http://docs.opencv.org/
[19] WiFly Library https://github.com/sparkfun/WiFly-Shield
[20] Technet.microsoft.com/en-us/magazine/jj554305.asps
[21] SHILPI CHANDNA, ROHIT SINGH and FAZIL AKHTAR, "DATA SCAVENGING THREAT IN CLOUD COMPUTING", International Conference on Computer Science and Mechanical Engineering, 10th August 2014, ISBN: 978-93-84209-42-1
[22] Ashish Bhagat, Ravi Kant Sahu, "Using Third Party Auditor for Cloud Data Security: A Review", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 3, March 2013.www.diablotin.com/librairie/networking/puis/ch06_05.htm by S Garfinkel - â€Ž1999
[23] Abhishek Mohta and Lalit Kumar Awasthi, "Cloud Data Security while using Third Party Auditor", International Journal of Scientific & Engineering Research,Volume 3, Issue 6, June-2012.

AUTHOR

Imran Hafiz Sayed received B.C.S degree in Computer Science from Maulana Azad College, Aurangabad, in 2011 and appeared for M.C.A degree in Computer Application from MarathwadaInstitute of Technology (MIT) in 2012.

Bhagyashree Brijmohansingh Rajput received B.C.S degree in Computer Science from Vivekanand College, Aurangabad, in 2012 and appeared for M.C.A degree in Computer Application from Marathwada Institute of Technology (MIT) in 2012.