IJITKM Volume 8 • Number 2 Jan-Jun 2015 pp. 15-19 (ISSN 0973-4414)

A Review of Security Techniques in Public Cloud Database

Pooja1, Dr.Dheerendra Singh2
Shaheed Udham Singh College of Engg, Tangori,Mohali, Punjab, India
vermapooja.2008@rediffmail.com, professordsingh@gmail.com

Abstract—Cloud computing is an on demand, Efficient, Convenient Network access to the all types of resources, like Software, Platform, Network resources, Data storage etc. As the data is stored on the Centralized server. So Security is the major issue in the cloud computing. The main Objective of this Paper is to Study and analyze the various techniques to prevent the attack from malicious users, by applying the various encryption techniques on the Database.

Keywords –Third party Auditor,Virtual machine, Fully homorphic Encryption

I. INTRODUCTION

Cloud computing is most revolutionary technique in the IT companies or even for individual users. This term is basically defined as the distribution of the resources over the internet.

Cloud computing is a model which enables convenient, efficient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. It is online technology, means till users are connected to the internet, they will be able to take benefits of the cloud computing. It provides benefits to the user like elasticity,Scalability,Reliability.cloud computing is under rapid development .

Architecture of Cloud Computing[1]:- Basically Cloud computing includes following entities:-

1.Customers: the entities who are using the services.

2.VM:VM stand for virtual Machine,which is the medium to make interaction between the customers and the CSP.

3.Cloud service Provider(CSP):CSP plays important role to upload the data of customers on the Virtual Servers.

4.Virtual Server:-Virtual server are the database servers on which database is actually sotred.

5.Third Party: Third party server is used to reduce the overhead of the CSP.

The two types of the models provided by the cloud computing are:-

Service models: Cloud computing provides services according to three fundamental models: Iaas(infrastructure as a service),Paas(platform as a service),Saas(Software as a service):-

1.**Saas(Software as a service):** This service model[2] enables customers to use the applications running on the cloud infrastructure. The applications are accessible by the customers through thin client inferface such as web browser. The consumer does not manage or control the underlying cloud infrastructure including network,server,operating system,storage or even individual application. The customers are aware of the coding behind the particular application.cloud computing provides the black box view of the applications means users are concerned with the only input and output. They can not control the way of functionality of the applications. It reduces the overhead of the customers.

2. **Paas (Platform as service):** This service provides the platform to the customers so that they can execute or deploy their applications on the platform provided by the cloud service provider.the customers have no control on the network,server,operating system,storage. But they can control their own applications on the platform.

3. **Iaas(Infrastructure as a service):-** The capability provided to the coutomer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Deployment models in Cloud computing:-

There are four types of clouds available in the cloud computing.Private,Public,Hybrid,and Community Cloud. These Deployment models[3] describe ,who owns,manages and is responsible for the services.

1.**Private cloud**: The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers(e.g. business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

2. Public cloud: The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or

government organization, or some combination of them. It exists on the premises of the cloud provider.

3. **Community cloud:** The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations) . It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

4. **Hybrid cloud:** Hybrid cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that will be unique entities, but bound together by standardized technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

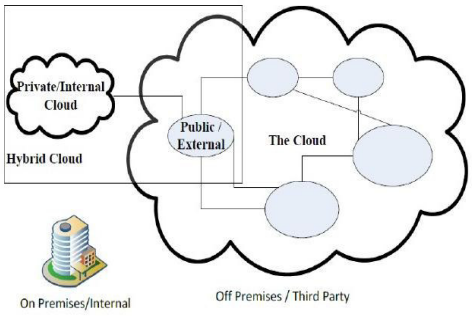

Figure 1 Deployment Models Of Cloud Computing[3]

II Literature Review

Security is the major concern in the cloud computing. Most of the bigger organizations feel insecure to give access of their data to the third party. And it is quite costly if they think to have their own cloud. lots of technologies has been applied to provide the more security in the cloud computing. The major issue in the security of cloud computing is the security in the cloud database. The different factors in the security of data are ,data integrity,data privacy affects in terms of encryptions techniques. Confidentiality can be achieved through encrypted storage[4][5][6][7].

1. The author Cong Wang et al. [8] used the public key based homomorphic authenticator and to achieve a privacy-preserving public auditing system for cloud data storage security while keeping all above requirements in mind, it uniquely integrate it with random mask technique.For efficiently handling multiple auditing tasks,the technique of bilinear aggregate signature can be explored to extend the main result into a multi-user setting, where TPA can perform multiple auditing tasks simultaneously. A keyed hash function hk(F) is used in Proof of retrievability (POR)[9][10] scheme. The verifier, pre-computes the cryptographic hash of F using hk(F) before archiving the data file F in the cloud storage, and stores this hash as well as the secret key K. The verifier releases the secret key K to the cloud archive to check the integrity.

2. **SUNDR[11]** stands for secure untrusted data repository. This is network file system which lets clients detect any modification by the malicious server. SUNDR Protocol achieves the property called Fork Consistency[27] which guarantees that cliens can detect any integrity or consistency failure by cryptographically protecting the file system, as long as they see each others modifications. The author jinyuan li implemented Serialized and Concurrent SUNDR in order to overcome the drawbacks of straw man file system, serialized SUNDR was used,in whichall files writable by the particular user are aggregated into single single hash value called i-hanle hash tree[28] and each i handle is tied to the latest version of every other i handle using version vector. I handles are stored in digitally signed messages known as version structure(VS). Each VS[29] must contain other user's i handle to which the user belongs.

In serialized SUNDR,each client must wait for previous client's version vector before computing and signing it's own. It will be beneficial for most operation to proceed concurrently, Where one User should wait for another ,when it reads a file,the other is in process of writing.

3. SPORC[13] is gerenal framework for building a wide variety of collaborative applications. SPORC provides a general collaborative services in which users can create a document, modify its access control, edit it concurrently experience fully automated merging of updated and perform these operations even while disconnected. SPORC provides the features of both OT[14] and Fork * consistency. SPORC includes application specific composition function which consolidated two operations i.e OT and Fork*consistency[25]. OT is used to recover from the Fork*consistency. Fork*consistency is used to detect the malicious server and clients . and OT is used to resolve from such attacks. OT Provides a general model for synchronizing shared state, OT allows each client to apply local updated optimistically when clients generate new operations then apply them through locally and then sending them to others. Each client accepts modification by others and apply them to locally. But the problem in OT may be due to order, to avoid this problem, transformation function was used.

The assumption in this paper is that the server is potentially malicious and misbehaving server.To prevent from malicious attack,clients in SPORC digitally sign all their operations with their user's private key.Digital signatures are not sufficient, because the server may still equivocate, to overcome this server equivocation, SPORC clients enforce Fork*consistency by maintaining hash chain over its view of committed history. Hash chain is

basically list of hash of its elements, H(.) is cryptographic function which is applied in this way like hi=H(hi-1||H(opi)) and || shows concatenation. And hi is value of hash chain over history upto opi.when a client with history upto opn submits new operation,it includes hn in its message. On receiving the operation,another clients check whether the included hn matches its own history, if they do not match, it means server is malicious.The server may be able to learn about which users and clients are sharing document, but it's not visible to them, what is in the document. SPORC supports large number of users and documents by replicating functionality. Clients are not trustworthy, They should not be able to see the state, modify user's authentication keys/(public/private) keys and access previleges. Hence the above procedure Detects the malicious server and attacks.SPORC provides two types of protocols one of them is based on the Key value store which means simple dictionary mapping string to string by applying simple transformation function. Last writer wins policy is used in the key value store and the Data type used in this is list of keys to update or remove and composite function to merge the list of keys. And the Second is based on the web based collaborative text editor,which allows multiple users to access,modify documents simultaneously like Google Docs[17] and ether Pad[18] to reuse data types and transformation composite function.

2.The author Luca Ferretti,Michele Colajanni and Mirco Marchetti "Distributed ,Independent and Concurrent Access to Encrypted Database [19] " provides the Secure DBaas to Protect the data from the unauthorized access or malicious users. Secure DBaas provides computations on the encrypted data. This paper provides three fold model i.e. Independent, Concurrent access to the geographically distributed clients in multi tenant form[22]. The SQL commands like Insert,Update,Delete are applied on encrypted data without intermediate proxy server. Because even a single Proxy server can cause any type of failure.This service acquires to install Secure DBaas on the client side and encrypted data will be sent through the network to Cloud service provider. The whole procedure is implemented through Emulab and network latency of applying the operations(SQL commands like Select, Insert, Update) on the plain text and encrypted text is compared.

III Results And Discussions

The runtime ,latency and throughput of the above three papers is compared in this section.

In SUNDR protocol, LFS small file benchmark is used to test SUNDR's performance on the simple file operations like Create, Read, Unlink. The acronyms used in the figure stands for:- NFS2 means Network File System version 2

NFS3 means Network File System version 3

SUNDR/NVRAM means SUNDR with Non Volatile Random Access Memory.

SUNDR only detects the attacks by fork*consistency. In the following figure comparison is shown between runtime for Create phase is shown:-

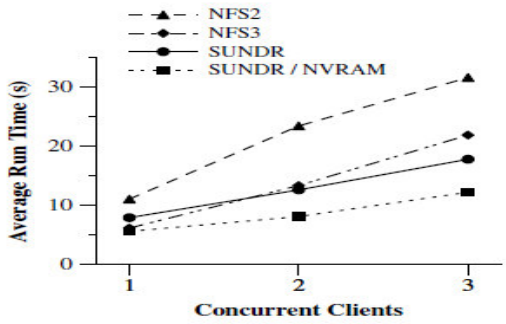

Figure 2: Concurrent LFS Small File Benchmark, Create phase.1000 creations of 1KB files[11]

In order to resolve the attacks, two types of SPORC protocols are used,SPORC with Key-value Store and SPORC with Text editor is used. OpenJDK Java VM (version IcedTea6 1.6) is used to implement the experiment. For RSA signatures, however the Network Security Services for Java (JSS) library from the Mozilla Project [26] is used. Both the protocols are implemented with high load condition i.e where 16 clients issuing write command.the large share of the cryptographic is due to the client side cryptographic operations and in text editor in text editor the latency is more due to the RSA signatures. It requires 10ms to compute a single signature.

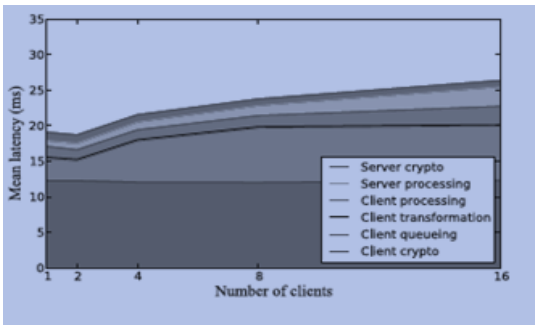

Figure 3: Loaded key-value store[13]

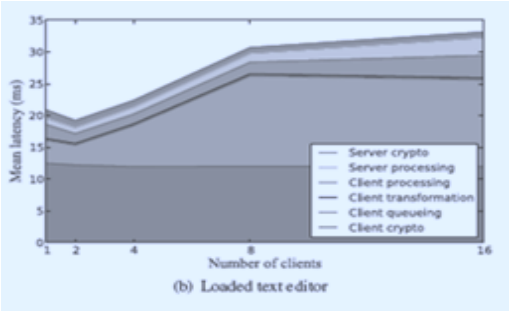

Figure 4: Loaded text editor [13]

In the Secure DBaas technique , TPC-C benchmark[24] is used to compare the level of performance. The whole experiment in is implemented on the Emulab.in the figure 5 , the comparison is shown between following three services:-

1.**Original TPC-C**: the standard TPC-C benchmark;

2.**Plain-SecureDBaaS**: SecureDBaaS that use all SecureDBaaS functions and data structures with no encryption.

3.**SecureDBaaS:** SecureDBaaS referring to the highest confidentiality level.

The network latency tend to mask the cryptographic overhead for any number of clients.there is decrease in network latency from 20%(40 concurrent clients with 40ms latecy) to 13%(40 concurrent clients with 80ms latency).

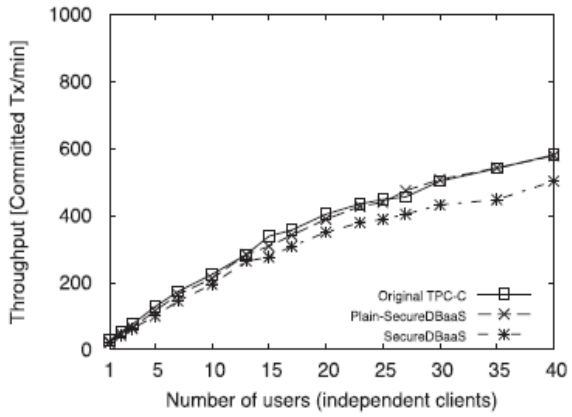

Figure 5: TPC-C performance (latency equal to 80 ms) [19]

IV CONCLUSION

To focus on the concept of Key management and Key sharing,We propose a scheme in which encryption will be applied to the data on the virtual machine and the keys will be stored and managed on the third party.Two algorithms will be applied in this scheme,DiffieHellman algorithm is applied to encrypt and decrypt the database by generating one time keys(Everytime the connection will be established,everytime new keys will be generated).HMAC algorithm is applied to ensure integrity by generating ticket to prevent man in middle attack in between user and virtual machine.

REFERENCES

[1] [May 2011] Qian Wang,Kui Ren,Wenjing lou and Jin li. "Enabling Public Auditability and Data Dynamics for Storage Security include Computing",IEEE transactions on Parallel and Distributed Systems Vol. 22, No.5

[2] [July 2013] Sanjoli Singla,Jasmeet Singh."Cloud Data Security using Authentication and Encryption Technique" IJARCET Vol 2 Issue 7.

[3] [Feb 2013] Bhavna Makhija,Vinit Kumar Gupta,Indrajit Rajput "Enhanced Data Security in Cloud Computing with Third Party Auditor" IJARCSSE,Vol. 3,Issue. 2

[4] [November 1993] Matt Blaze "A cryptographic file system for Unix",ACM conference on Communications and computing Security, pages 9-16

[5] [February 2003] Eu-Jin Goh, Hovav Shacham, Nagendra Modadugu, and Dan Boneh. SiRiUS: Securing Remote Untrusted Storage. In Proceedings Symposium,Internet Society (ISOC),Pages 131-145

[6] [April 2003],M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu.Plutus: Scalable secure file sharing on untrusted storage. In 2nd USENIX conference on File and Storage Technologies San Francisco, CA of the Tenth Network and Distributed System Security (NDSS) (FAST '03)

[7] [June 2003],Charles P. Wright, Michael Martino, and Erez Zadok.
NCryptfs: Asecure and convenient cryptographic file system. In Proceedings of the Annual USENIX Technical Conference, pages 197–210

[8] [March 2010] Cong Wang,Qian Wang and Wenjing Lou,"privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing"IEEE Infocom,SAN Diego,CA.

[9] [2007] A Juels and B.Kaliski Jr.,"Proof of retrievability for Large Files",ACM Conference. Computer and Comm.Security

[10] [2008], H.Shacham and B Waters,"Compact Proofs of retrievability",ASIACRYPT.

[11] [Oct 2004],J Li,M.Krohn,D.Mazieres and D.Shasha,"Secure Untrusted Data Repository", USENIX Association OSDI '04: 6th Symposium on Operating Systems Design and Implementation

[12] Russel Sandberg, David Goldberg, Steve Kleiman, Dan Walsh, and
Bob Lyon. Design and implementation of the Sun network filesystem.
In Proceedings of the Summer 1985 USENIX Portland, OR, 1985. USENIX. pages 119–130

[13] Ariel J.Feldman,William P.Zeller,Michael J.Freedman and Edward W.Felton Princetone University "SPORC,Group Collaboration using Untrusted Cloud Resources"

[14] [1989],C. Ellis and S. Gibbs. Concurrency control in groupware systems. ACM SIGMOD Record, 18(2):399–407

[15] Prince Mahajan,Srinath Setty,Sangmin Lee,Allen Clement,Lorenzo Alvisi,Mike Dahlin, and Michael Walfish,"DEPOT:Storage with Minimal Trust",The University of Texas at Austin

[16] [October 1997] M. Handley and J. Crowcroft. Network text editor (NTE) "A scalable shared text editor for MBone. In Proc. SIGCOMM"

[17] [2010],Google. Google Docs. http://docs.google.com/

[18] [2010],Google. EtherPad. http://etherpad.com/

[19] [February 2014] Luca Ferretti, Michele Colajanni, and Mirco Marchetti," Distributed, Concurrent, and Independent Access to Encrypted Cloud Databases,IEEE Transactions on Parallel and Distributed Systems,Vol.25,No.2

[20] [2005] US Secret Service Report on insider attacks. http://www.sei.cmu.edu/about/press/insider-2005.html.

[21] [2012] Huaglory Tianfield,School of Engineering and Built Environmet,"Security Issues in Clud Computing", IEEE International Conference on Systems,Man and Cybernetics.

[22] [February 1999.] Miguel Castro and Barbara Liskov. Practical byzantine fault tolerance.In Proceedings of the 3rd Symposium on Operating Systems Design and Implementation, pages 173–186, New Orleans, LA,

[23] [October 1991],M. Rosenblum and J. Ousterhout. The design and implementation of a log-structured file system. In Proceedings of the 13th ACM Symposium on Operating Systems Principles Pacific Grove, CA, ACM, , pages 1–15,

[24] [Apr. 2013]" Transaction Processing Performance Council," TPC-C, http://www.tpc.org

[25] [April 2007],J. Li and D. Mazi`eres. Beyond one-third faulty replicas in Byzantine fault tolerant systems. In Proc. NSDI

[26] [2010], Mozilla Project. Network security services for Java (JSS). https: //developer.mozilla.org/En/JSS

[27] [July 2002],David Mazi`eres and Dennis Shasha. Building secure file systems out of Byzantine storage. In Proceedings of the 21st Annual ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing,pages 108–117

[28] Ralph C. Merkle. A digital signature based on a conventional encryption function. In Carl Pomerance, editor, Advances in Cryptology—CRYPTO '87, pages 369–378

[29] 1987. Springer-Verlag. , volume 293 [May 1983], D. Stott Parker, Jr., Gerald J. Popek, Gerard Rudisin, Allen Stoughton, Bruce J. Walker, Evelyn Walton, Johanna M. Chow, David Edwards, Stephen Kiser, and Charles Kline. Detection of mutual inconsistency in distributed systems. IEEE Transactions on Software Engineering, SE-9(3):240–247