Volume 4, Issue 1
February 2015

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

Comparative Study and Improved Security Threats in Cloud Computing

[1]Iram Matloob, [2]Tauqeer H. Shah [3]Syeda Hina Batool, [4]Momena Aamir

[1]Lecturer Department of Software Engineering, Fatima Jinnah Women University Pakistan

[2]Area Facilities Engineer, Harouge Oil Operations Libya

[3]Undergraduate Student, Department of Software Engineering, Fatima Jinnah Women University Pakistan

[4]Undergraduate Student, Department of Software Engineering, Fatima Jinnah Women University Pakistan

[1]irummatloob@yahoo.com, [2]tauqeer@iee.org, [3]syedahb14@gmail.com, [4]mona.cool93@gmail.com

ABSTRACT

Data security is the fundamental issue of all information systems. In cloud computing environment data security is a serious issue because data is distributed and scattered in various places. Though a lot of work is done in order to provide secure cloud environment, data security is still the main hurdle in the development of this system. This paper reviews various security challenge and techniques to solve security issues in order to achieve data protection in cloud environment. In this paper we have done a comparative analysis of existing research in the field of cloud computing data security and privacy.

Keywords: Cloud Computing, Data Integrity, Data Confidentiality, Unauthorized Access, Data Availability.

1. INTRODUCTION

Cloud Computing is the most promising computer prototype in the IT world that provides services in the form of on demand basis. Although cloud computing is still a developing field of IT, this idea has been around for a couple of years. It is named as cloud computing because applications/information exists on a cluster of "cloud" of Web servers. It is accessible by everyone, from everywhere and at any time, together with the clouds related to web and internet. In simplest terms, it is the practice of storing and accessing information and data over the internet rather than one's own local server or a personal computer. The main objective of cloud computing is to provide accessible and economical on-demand computing setups with good quality of service levels.

Cloud infrastructure has massive advantages. The most vital one is that the clients don't need to buy the resource from a third party vendor, as an alternative they can use the resource and pay for it as a facility or a service. In this way it helps the client to save time and money.

The advantages of this technology are pretty tempting, but nothing comes without a cost. This new setup has its drawbacks like all computer systems. A critical drawback that decreases the trust between the customer and the service provider is the security, especially the data theft,

privacy and data loss. The major concern of companies and corporate individuals is how security and integrity can be managed in the cloud. Open systems and shared resources elevate many security related threats, thus making security a major obstacle to adopt cloud computing architecture. An IDC survey is conducted by the IT executives and according to that survey the most critical issue in this environment is security (as shown in the results given below)[1]. Moving sensitive data and information to public cloud is the major issue because this data is under the supervision of a third party (Service Provider).

TABLE I

CLOUD ISSUES AS PER IDC

Rate the challenges or issues of cloud as per IDC survey This paper emphasis on some papers that indicates different security challenges that users have to face in the cloud and review various security techniques for privacy and protection in cloud.

ITEE Journal
Information Technology & Electrical Engineering

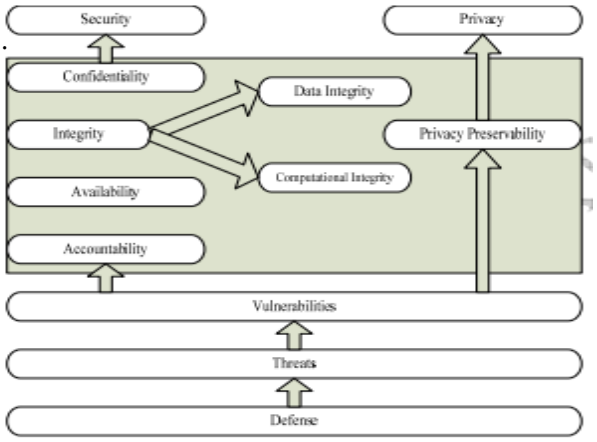
ISSN: - 2306-708X

Security	87%
Availability	83%
Performance	82%
On-demand Payment Model Cost More	81%
Lack of Interoperability Standards	80%
Bringing back to in-house may be difficult	79%
Hard to integrate with in-house IT	76%
Not enough ability to customize	76%

This paper firstly explores the security issues in the cloud in section 2. Then in section 3 it reviews some of the existing techniques and solutions to avail security in cloud.

2.SECURITY ISSUES IN CLOUD COMPUTING

Security threat is a critical issue for cloud consumers and producers . Cloud environment has wide variety of threats because of the blend of several technologies. Some of the security issues relating to data confidentiality, data privacy, data integrity and data availability are discussed below



A. Data Confidentiality

Data Confidentiality is an important factor for cloud users because it helps them to protect their private or confidential data and keep it safely in cloud. Authentication and other access restriction strategies are used to ensure unauthorized data disclosure prevention. Cloud Service Providers are unable to completely eliminate the threats and hackers attacks. Encryption is done on a medium level but this is not enough as far as the complex requirements like object level security, commands and other changing's are concerned so to meet the challenges of increasing technology precariousness its really important to increase the level of authorization and reliability of cloud.

B. Data Privacy

Privacy is the ability of an individual or a group to protect the information and assets regarding him or itself and revealing a proportion of it if needed. it is a trait in which a person maintains the confidentiality of his information.

In cloud the privacy means when users access their data, the systems prevent other users to access that data ambiguously from a remote server, which means the data can be only accessed by a single person who is authorized to do so.

The privacy issues related to cloud can be categorized into following 4 classes

1.How to provide users control of their data stored in cloud and how to avoid unauthorized access of this information.

2.How to provide secure data replication and evade leakage, data loss, alteration or fabrication.

3.Which party ensure legal requirements for private data.

4.The level of involvement of cloud sub contractors for the proper processing of data.

Some of the major issues which cloud consumers and producers have to face regarding privacy are as follows:

1) Service Abuse*:* In general term it means cloud users are abused by other users. Attackers gain access of extra data and demolish the interests of other users. Service providers must avert service abuse.

2) Identity Management: Cloud computing provide many services to its users but beside this its increases the security risk. This risk increases when trusted third group get involved, due to the inclusion of third group the number of heterogeneous group of users 'increases that ultimately result in increase in risky situation. The solution to this problem is that service providers must separately deal with that third trusted group and manage the identity of third group independently.

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

3) Averting Attacks: Cloud computing service provides customers to share large amount of resources on internet. Cloud system should not allow Denial of Services attack.

C. Data Integrity

For any information system, data integrity is the key element. In general term, data integrity means , keeping data secure from unauthorized modification, fabrication and deletion. In a stand alone system data integrity is easily implemented using a relational database. DBA (Database Administrator) maintain data integrity through database constraints and transactions. All transactions should follow ACID.

In cloud computing data integrity means protecting integrity of information. The information should not be fabricated or lost by unauthorized users. Data integrity in cloud is fundamental requirement for the provision of services such as Saas, Paas and Iaas.

Integrity issues instantly crop up when databases related to cloud computing are analyzed. Middlewares that connect systems to cloud uses the structures or rules applied in databases being connected. So there is a critical threat of integrity loss if relationships are not correctly defined. Some databases have built in integrity controls while mostly when connected to cloud require application techniques to acquire integrity. But unfortunately all this is not easy to achieve and become much complex when considering the fact that cloud computing system is widely distributed. It becomes quite tricky to create common mechanism to control integrity.

D. Data Availability

It refers to the term used by computer storage manufacturers and the storage service providers to describe the products and services which ensure that data will continue to be available even in situations like "Disastrous" or "Catastrophic" failures at a maximum level of required performance .It also means that how user data can be recovered and verified using different techniques rather than depending upon the cloud services.

Storing data on central location is a big concern of clients because cloud purveyors are controlled by local laws, so therefore cloud clients should be intimated of those laws In turn the cloud service providers should ensure data authenticity, data safety and data secrecy .The cloud service providers should show concern in the availability of these ministrations and incorporate a certitude relationship with customers in this analogy. The cloud purveyor should provide assurance of safety of data and explicate the power of the local laws to the clients.

Some of the common issues regarding availability are as follows:

1) Data Recovery : All information in cloud is stored in hardware devices. Data backup is maintained by service providers. Data and its backup may be stored on same device. This will be a critical problem in case of any sort of disaster. Cloud clients must sort out these issues with the providers and service providers must provide data availability in case of any sort of disaster.

2) Reliable Storage Agreement **:**An untrusted storage shows an unusual behavior in which cloud service providers toss out the updated part of the user data which cannot be recovered by simple encryption techniques. And a good storage should support concurrent modifications by multiple users. Cloud providers must ensure the reliability of the storage by incorporating any available technique.

3.SOLUTIONS OF THE SECURITY ISSUES

In this section some of the existing techniques and solutions have been discussed and compared in order to acquire data confidentiality, data privacy, data integrity and data availability in cloud computing environment.

A. Hemomorphic Encryption

It is a type of encryption basically carried out on Cipher text using cipher text algorithm which gives an encrypted result and when decrypted it matches with the operations performed on plaintext. It involves very complex computations and In cost and Benefit analysis context this technique is not as much effective because it has a high cost of computing and storage [2].A cryptography mechanism was used also used but to increase reliability and flexibility, a hybrid technique that involves a combination of encryption algorithms such as RSA, 3DES, and random number generator has been proposed[3].

B. Encrypted Search Database

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

In response to the inefficiency of homomorphic encryption, encrypted database mechanism is introduced but it has a drawback that as the number of keys get increased the number of computations also become more complex and large[4]. Another technique called memory database encryption key also becomes the part of it in which a synchronizer act between the owner and client and the client receive key to decrypt data from owner it has a limitation that delays occur due to extra communication with the synchronizer .This limitation can be handled by avoiding extra communication with the synchronizer and making group encryption[5].

C. Distributive Storage

To maintain the data consistency and accuracy Distributive Storage approach is used in which data is divided into chunks these chunks are then encrypted and stored in separate databases, thus called distribution of data over cloud and hence provides intensified security against different threats[6].

D. Hybrid techniques

It is a three layered technology used for the data integrity and authentication. The first layer authenticates the cloud users, the second layer is used for the encryption of cloud user data and the third layer then decrypts the data quickly[7].

E. Data Concealment: In this encryption technique real or actual data is combined with fake data so that counterfeit data can easily be separated but authorized users can differentiate between the two, it is used to increase and enhance the security and prevent data from hackers and stealers of the data. Watermarking key is used for this purpose, only authorized users have an access to this key so to make sure that authentic users have an access to the real data[8].

F. POR (Proof Of Retrieveability): It is a protocol in which server/cloud ensures its client that the file F is undamaged and is not modified by the cloud and user can retrieve it . This techniques is used to ensure the integrity of the data. POR is named as sentinels for large size of F. When user challenge the cloud server to check integrity, the response protocol server will send a subset of the sentinel. If information is fabricated , the sentinel will be lost and the server cant make the copy or proof of F. In this way user/ client get to know that the original file is modified[9].

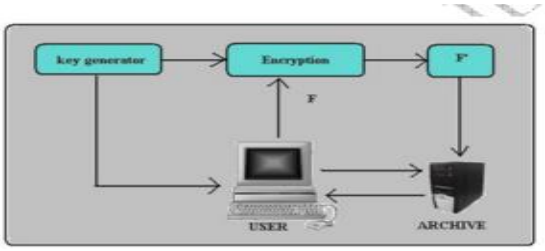


Fig 2. Schematic view of POR

G. PDP (Provable Data Possession)

This model is given by Ateniese et al. This model is used to check the availability and integrity of data which is stored in cloud . Using this technique client can confirm that the untrusted server has the original unmodified data without keeping the copy of data or retrieving it.PDP uses cryptographic hash functions and symmetric key encryption[10].

H. FADE System

When user delete the data from cloud it should not be recovered by the unauthorized users. So in order to completely delete the data FADE system was proposed[11]. It uses Ephemerizer technique. According to it, data is encrypted before uploading .When user wants to delete the data it will be deleted from all places in the database and the new data is replaced with the deleted data.

I. SPORC

This technique is used to ensure the data availability in cloud. It provides an interactive and effective collaboration for multiple users in a safe cloud storage environment and untrusted cloud servers can only view the encrypted information. However the techniques proposed have limitations and can only occur on client end.

J. HAIL

The HAIL technique deploy POR mechanism to check the information storage in multiple clouds. It does the

availability and integrity checking of the data and also ensures the data redundancy of various copies. Schiffman et al proposed TPM (Trusted Platform Module) for the remote checking of data integrity.

4. CONCLUSION

Cloud computing is the most happening and promising technology which will change the future of IT world. The barrier towards the growth of cloud computing is data security and privacy. Reduction in data storage cost is the fundamental requirement for any organization but no organization will compromise on security of its sensitive data which is needed for decision making. So no organization will acquire the services of cloud until trust is built between the clients and cloud service providers. Researchers have done a lot of work and proposed many techniques to protect data in cloud and to achieve a high level of security. However there is still a room for improvement in order to make cloud fully secure by making techniques more effective. To fully satisfy the cloud consumers more work is required in this field. This paper surveyed existing techniques for data security and data protection in cloud computing which can be deployed in cloud computing environment in order to build trust between cloud consumers and service providers.

REFRENCES

[1] N. Kshetri, "Privacy and security issues in cloud computing: the role of institutions and institutional evolution,".

[2] R. L. Rivest, L. Adleman, and M. L. Dertouzos, "On data banks and privacy homomorphisms,"Foundations of Secure Computation, vol. 4, no. 11, pp. 169–180, 1978.

[3] C. Gentry, A fully homomorphic encryption scheme [Ph.D. thesis], Stanford University, 2009.

[4] D. Manivannan and R. Sujarani, "Light weight and secure database encryption using tsfs algorithm," in Proceedings of the International Conference on Computing Communication and Networking Technologies (ICCCNT '10), pp. 1–7, IEEE, 2010.

[5] F. Pagano and D. Pagano, "Using in-memory encrypted databases on the cloud," in Proceedings of the 1st IEEE International Workshop on Securing Services on the Cloud (IWSSC '11), pp. 30–37, September 2011.

[6] C. P. Ram and G. Sreenivaasan, "Security as a service (sass): securing user data by coprocessor and distributing the data," in Proceedings of the 2nd International Conference on Trendz in Information Sciences and Computing, (TISC '10), pp. 152–155, IEEE, December 2010.

[7] A. Rao, "Centralized database security in cloud," International Journal of Advanced Research in Computer and Communication Engineering, vol. 1, pp. 544–549, 2012.

[8] C. Delettre, K. Boudaoud, and M. Riveill, "Cloud computing, security and data concealment," in Proceedings of the 16th IEEE Symposium on Computers and Communications (ISCC '11), pp. 424–431, Kerkyra, Greece, July 2011.

[9] R. Sravan and Saxena ,"Data integrity proofs in cloud storage" in IEEE 2011.

[10] R. Pandya, K. Sutaria, "An analysis of privacy techniques for data integrity in the cloud environment", International Journal of Computer and Electronics Engineering,(Dec 2012) ISSN: 0975-4202

[11] Y. Tang, P. P. C. Lee, J. C. S. Lui, and R. Perlman, "Fade: secure overlay cloud storage with file assured deletion," in Security and Privacy in Communication Networks, pp. 380–397, Springer, New York, NY, USA, 2010.

Volume 4, Issue 1
February 2015

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

Author Profiles:

Irum Matloob:
She has earned BSc & MSc software engineering degrees, and she is a lecture at Fatima Jinnah Women University and previously she was a lecturer in Foundation University.

Tauqeer H. Shah:
He earned B.Sc electrical engineering from FUM and M.Sc electrical engineering from IUST, currently working with Harouge Oil Operations Libya (Joint Venture of NOC Libya and Petro Canada) as a Lead Area Facilities Engineer at Ghani Field, overall having 19 years of Oil & Gas field experience. Having corporate membership of (IET) Institution of Engineering & Technology London United Kingdom and currently also working with IET as an international professional registration advisor (IPRA). Received professional qualifications of (C.Eng) Chartered Engineer from institution of engineering & technology through Engineering Council United Kingdom.

Syeda Hina Batool:
She did her matriculation from Army Public School and College for Girls, Rawalpindi. The she did FSc from F.G College for Girls, Kashmir Road Rwp. She is currently doing Software Engineering from Fatima Jinnah Women University, Rawalpindi and is in 6th Semester.

Momena Amir:
She did her Matriculation from Army Public School, Hamayun Raod. The she did her FSc from Punjab College. She is currently studying in Fatima Jinnah Women University and doing Software Engineering. She is in 6th semester.