International Journal For Technological Research In Engineering *ISSN (Online): 2347 - 4718*
International Conference on Emerging Technologies in Engineering, Biomedical, Medical and Science (ETEBMS - November 2016)

A REVIEW OF MAJOR SECURITY ISSUES IN CLOUD COMPUTING

Mitesh Sharma
Assistant Professor, Department of CSE, JIET College of Engineering

Abstract: In the current era cloud computing is acquiring great deal of attention in users, markets, education and publications. Cloud is a group of servers that provide highly scalable services like SaaS, PaaS, IaaS to transform computing in business. Information stored in clouds is accessible from anywhere at any time. Cloud providers have storage, software and infrastructure facilities to run businesses effectively. Cloud computing is a dominant technology that facilitates businesses to become more connective, scalable, collaborative, real-time and productive. Cloud computing is based on the concept of virtualization and hence eliminates the need of a powerful configuration deployment by providing services at a reasonable price and hence this technology is very helpful for small organizations that cannot afford the cost of infrastructure and storage space. This robust technology has shifted the cost of managing hardware, software and computational infrastructure to third parties such as Google, Microsoft, Amazon. By shifting the costs of managing computational infrastructure to third parties, cloud computing has made it possible for individuals and small organizations to deploy world-wide services; all they need to pay is the marginal cost of actual resource usage. There are number of users used cloud to store their personal data, so that data storage security is required on the storage media. The major concern of cloud environment is security during upload the data on cloud server. Data storage at cloud server attracted incredible amount of consideration or spotlight from different communities. For outsourcing the data there is a need of third party. The importance of third party is to prevent and control unauthorized access to data store to the cloud. This research paper starts with introduction to the cloud computing. After that the service models and the deployment models are being discussed to create a basic understanding of the implementation level details of cloud computing. Thereafter the characteristics of cloud computing are discussed which is being followed by the security issues of cloud storage..

I. INTRODUCTION

THECloud Computing has changed the way how people use technology without investing in new infrastructure facilities, training new personnel or procuring new software. Cloud is an impactful technology that provides on-demand access to computing resources at a marginal and predictable cost. Cloud computing is a recent dominant technological development widely accepted by organizations, educational institutions and individual users. Cloud computing adds a new dimension to business models by eliminating the need of a powerful physical configuration. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications. Cloud storage specifies the storage on cloud with almost inexpensive storage and backup option for small enterprise. The actual storage location may be on single storage environment or replicated to multiple server storage based on importance of data. The mechanism model of cloud storage consists of four layers: storage layer which stores the data, basic management layer which ensures security and stability of cloud storage itself, application interface layer which provides application service platform, and access layer which provides the access platform.

II. CLOUD COMPUTING

A. Understanding Cloud Computing

Users connect the cloud they seen cloud as a single application, device, or document. All things inside the cloud system like hardware in the cloud and the operating system that manages the hardware connections are invisible. Cloud computing starts with the user interface seen by individual users. This is how users gives their request then gets passed to the system management, which finds the correct resources and then calls the system's appropriate provisioning services. Cloud computing is mainly used for data storage. Here the data is stored on multiple third-party servers. The user sees a virtual server; it appears as if the data is stored in a particular place with a specific name, when storing the data. This doesn't exist in reality. It's just used to reference the virtual space of the cloud. In reality, the user's data could be stored on any one or more of the computers used to create the cloud.

B. Cloud Computing Service Models

Cloud Infrastructure as a service (IaaS): In this composition of implemented environment for their system a supplier must be supply a different computing resources which include loading, processing unit. Client has flexile to achieve and switches a softwaremultilated to be implemented and vary between different applications like operating system etc. There are different issues in IaaS such as:

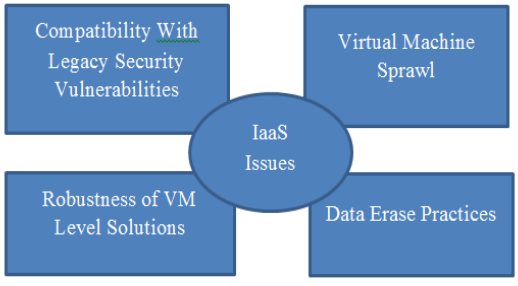

Figure 1

Cloud Platform as a service (PaaS): This software supplies client with the ability to establish and extended applications that are mainly positioned on equipment and programming languages promoted by the suppliers. In this the client has no containment over the different organization but has containment over the extended applications. Examples of this class of services include Google App Engine, Windows Azure Platform and rack space. There are different issues in PaaS such as:

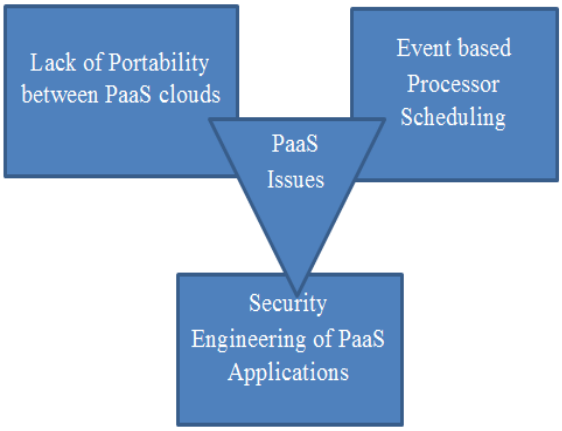

Figure 2

Types of PaaS:

There are different types of PaaS such as

- Application Delivers onlyEnvironments
- Standalone DevelopmentsEnvironments
- Open Platform & OpenService
- Add on DevelopmentPossibility

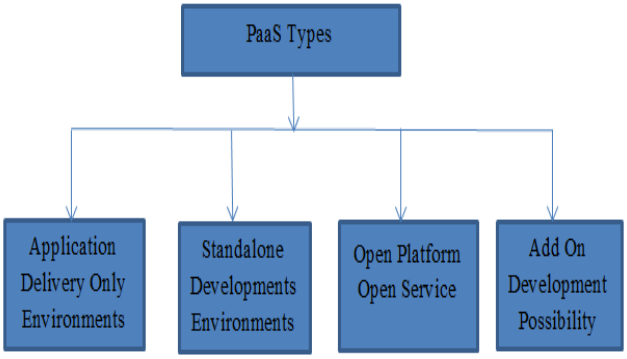

Figure 3

Cloud Software as a service (SaaS): This software supplies the ability to usage the appliances which implemented on cloud organization. With the usage of standard interfaces like web browser or online(e-mail) client, these appliances are obtainable. SaaS appliances are obtained from different devices like mobile, workstation from anywhere at any time.

Cloud Network as a service (NaaS): NaaS provides the capability to use the network services and inter-cloud network connectivity services. Improvement of possession allocation services include in view of network and computing resources. These type of services involved extensible, enhanced virtual private network.

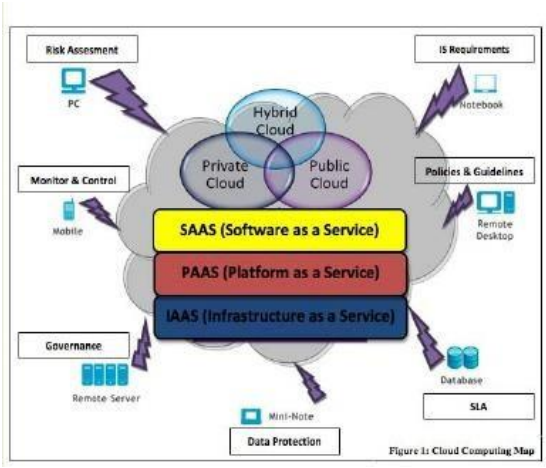

Figure 4

C. Cloud Computing Deployment Models

The security issues starts with the cloud deployment models. Depending on infrastructure ownership, there are four deployment models of cloud computing.

- The Public Cloud: Which describes cloud computing in the traditional mainstream sense; resources are dynamically provisioned on a self-service basis over the Internet. It is usually owned by a large organization (e.g. Amazon, Google's App Engine and Microsoft Azure).This is the most cost-effective model leading to user with privacy and security issues since the physical location of the provider's infrastructure usually traverses numerous national boundaries.
- The Private Cloud: It defers from the traditional data enter in its predominant use of virtualization. It is a single tenant environment. They have been criticized on the basis that users still have to buy, build, and manage them and as such do not benefit from lower capital costs and less hands on management. The private cloud is more appealing to enterprises especially in mission and safety critical organizations.
- The Community Cloud: Thus refers to a cloud infrastructure shared by several organizations within a specific community. It may be managed by any one of the organizations or a third party. A typical example is the Open Cirrus Cloud Computing Testbed, which is a collection of Federated data centres across six sites spanning from North America to Asia.
- The Hybrid Cloud: It comprises of a combination of any two (or all) of the three models discussed above.

Standardization of APIs has lead to easier distribution of applications across different cloud models.

III. CLOUD COMPUTING CHARACTERISTICS

On Demand self-service: A cloud might individually attain computing possibilities, as per the use of different servers, network storing, as on request, without communicating with cloud provider.

Broad Network Access: Services are delivered across the Internet within a standard mechanism and access to the services is possible through assorted customer tools.
Resource pooling: A multitudinous model is employed to serve different types of clients by making pools of different computing resources, as per the request of customers these have different resources which can be assigned and reassigned dynamically.
Rapid Elasticity: Capabilities might be elastically provisioned or rapidly released. From customers view, the provided possibilities come out to be limitless and must have the capability to purchase in any quantity at any time.
Measured Services: The provision procured by different clients is measurable. The use of asset will be directed, estimated, and accused for contributor and asset.

IV. SECURITY ISSUES

TRUST

Trust between customer and service providers is the main issue faced by cloud computing now days. Customer is never sure whether the Service is trustworthy or not, and whether his data is secure from the intruders or not. The customer and Service provider are bound by Service Level Agreement (SLA) document. This is a type of an agreement between the customer and the service provider; it contains the duties of service provider and his future plans. But unfortunately there are no standards for SLA.
Many efforts have been made till now to resolve the issues of trust and privacy to resolve the security issues in cloud. A trust model is presented in to enhance the security and interoperability of cloud computing environment. Husky Healthcare Social Cloud presents a trust rating mechanism to secure the cloud environment in collaboration with social media. SLA Framework is used in to propose a trust management model for security in cloud environment.

CONFIDENTIALITY

Confidentiality means to prevent the disclosure of private and important information. Since all the information is stored on geographically dispersed locations, confidentiality becomes a big issue. Many methods are used to preserve confidentiality from which, encryption is the widely used method. But it is relatively an expensive method.
To preserve privacy, a secure cloud storage service is designed that is built upon the public cloud structure and by using cryptographic techniques, privacy is achieved. A new approach proposed by uses hierarchy of P2P reputation system to preserve privacy. It gains it with virtualized defense. Describes that the attribute-based cryptography can be used to preserve privacy and maintain security in a cloud based EHR system and patients can sharedatainaflexible, scalableanddynamicmanner.

AUTHENTICITY

Integrity is also a main issue faced by cloud computing. It refers to the improper modification of information. As the data resides in different places in a cloud so the access control mechanism should be very secure and each user must be verified as an authentic user.
Authentication problem can be solved by using the digital signatures but even after having access to digitalsignatures a user can't get access and verify the subsets of data.
An access control scheme presented by is a decentralized and robust access control mechanism where the cloud user identity is verified by the cloud without knowing the user's identity before storing information. Information can be decrypted by only the authentic users. Replay attacks are also prevented in this scheme. Another scheme new setting is presented where the users are independent from the service providers and they don't need to register with them. Data owner provides the user the credential information. The username and password pair generates the identity information for each user that is provided to the service provider by the data owner. This scheme proves to be very scalable.

ENCRYPTION

Encryption is the most widely used data securing method in cloud computing. It has many drawbacks. It needs high computational power. The encrypted data need to be decrypted every time when a query is run so it reduces the overall database performance. Many methods are presented to ensure better encryption in terms of better security or the operations.
A method proposed by suggests that by using several cryptographic methods instead of only one can increase the overall throughput. Data is encrypted using these methods in each cell of a table in cloud. Whenever a user wants to make a query, the query parameters are evaluated against the data stored. The query results are also decrypted by theusernottheclouditselfsoitincreases the overallperformance.
Another method called end-to-end policy based encryption uses different policies to encrypt and decrypt data. The decryption keys are released by the Trust Authority enabling a user to get fine grained access control in public clouds.
Another approach called fully Homomorphic encryption is a new trend that can provide results of calculation performed on encrypted data rather than the raw data. It increases the data confidentiality and better encryption.

KEYMANAGEMENT

While doing encryption, we need encryption/decryption keys and managing these keys itself is a big security issue in cloud environment. Storing these encryption keys on cloud is a bad option. It is easy to store single encryption key but for the real time systems it become a complex task to store these keys. This may require a separate small database to store the keys locally in a protected database. But again that's not a good idea because the purpose for which we are shifting our data to clouds will become worthless. As by doing so we will need additional hardware and software resources and the cost issues will also arise. The only solution to key management may be through two-level encryption [25]. This can be very helpful to store encryption keys incloud.

DATASPLITTING

Data splitting may be the better alternative to encryption.It is

surely very fast as compared to encryption itself. The main idea behind it is to split the data over multiple hosts that are non-communicatable. Whenever a user needs its data back, he must have access to both of the service providers to recollect his original data. No doubt it is very fast technique but it has its own security issues.

Multi-Cloud Database Model [7] is a method for data splitting where multiple clouds and different techniques are used to ensure the integrity and availability of data after splitting it. In this way the security is very much enhanced as the data is stored and replicated in multiple clouds and there are fewer chances of the intruders to attack. These clouds share data using secret sharing algorithm and TMR technique.

MULTITENANCY

In a cloud environment, different resources and services are shared among different applications at different geographic locations. This is done to solve the issues of resource scarcity and to eliminate cost that is the main purpose of the cloud. But the sharing of the resources of an organization gives birth to confidentiality issues. These systems and applications must be isolated to some extent in order to keep confidentiality alive. Otherwise it is very difficult to supervise the data flow and the insecurity issues arise.

Data and applications in a cloud may be stored on virtual servers as well as on the actual hardware. In both of the cases there are security issues involved. If these are stored virtually, there are chances that one virtual machine hosting a malicious application can affect the performance of other machines. If these are stored on actual hardware, there may be security issues because of multi-core processing.

Cloud providers should employ Intrusion Detection Systems to keep their customers safe in cloud environment. Architecture to deploy IDS is presented in. Trusted cloud computing platform (TCCP) is designed to provide better security of the virtual machines.

V. CONCLUSION

Cloud computing by itself is in evolving stage and hence the security implications in it aren't complete. It is emerging as the various organizations that are developing cloud services are evolving. It is evident that the Even the leading cloud providers such as Amazon, Google etc are facing many security challenges and are yet to stabilize. Achieving complete solution for legal issues is still a question. With this level of issues in cloud computing, decision to adopt cloud computing in an organization could be made only based on the benefits to risk ratio. Cloud must be safe from all the external threats, so there will be a strong and mutual understanding between the customer and the cloud service provider. The largest comes when the differences between actual cloud security and virtual machine security comes. Research should be center on these gaps and differences and its removal. Main goal of cloud computing is to securely store and manage the data in cloud. One solution for cloud security issues is to produce the framework might be developing a way to monitor the cloud's management software, and another might bedevelopment of isolated processing for specific clients‟ applications. It is useful to track the client's behaviour andmonitored for instance whether client allow the updating anti-virus software definitions , or ,automated patching software to run, or whether client understand how to make safe their virtual machines in the cloud. Cloud computing is relatively a new and widely emerging domain and it must have to over come the security issues in order to be more and more prominent technology of the future. A lot of research is being done in this regard to solve these major issues but still many problems are unseen and unknown and the doors for future research are always open.

REFERENCES

[1] Messmer, Ellen (March 31, 2009). "Cloud Security Alliance formed to promote best practices". Computerworld.Retrieved May 02, 2014.

[2] "Security Guidance for Critical Areas of Focus in Cloud Computing". Cloud Security Alliance. Retrieved May 02, 2014.

[3] Li, Wenjuan, and Lingdi Ping. "Trust model to enhance security and interoperability of cloud environment." In Cloud Computing, pp. 69-79. Springer Berlin Heidelberg, 2009.

[4] Kant, DrChander, and Yogesh Sharma. "Enhanced Security Architecture for Cloud Data Security." International Journal of Advanced Research in Computer Science and Software Engineering 3.5 (2013):571-575.

[5] RajkumarBuyya, Chee Shin Yeo, SrikumarVenugopal, James Broberg and IvonaBrandic, "Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility," Future Generation Computer System, 2009, pp. 599-616.

[6] Ren K, Wang C, Wang Q (2012) Security challenges for the public cloud. IEEE Internet Comput 16(1):69–73.

[7] AsmitaPandey, ―Cloud Computing – An on Demand Service Platform‖, International Conference on Advances in Management and Technology (iCAMT - 2013) Proceedings published in International Journal of Computer Applications® (IJCA) (0975 – 8887).

[8] Mohiuddin Ahmed, Abu Sina Md. RajuChowdhury, Mustaq Ahmed, Md. MahmudulHasanRafee, ―An Advanced Survey on Cloud Computing and State-of-the-art Research Issues‖, IJCSI International Journal of Computer Science Issues, ISSN (Online): 1694-0814, Vol. 9, Issue 1, No 1, January 2012.

[9] JueeU.Daryapurkar, Prof. Karuna G. Bagde, ―Cloud Computing: Issues and Challenges‖, International Journal on Recent and Innovation Trends in Computing and Communication, Volume: 2 Issue: 4 770 – 773.

[10] Problems Faced by Cloud Computing, Lord CrusAd3r,dl.packetstormsecurity.net/.../ProblemsFa

cedbyCloudComputing.pdf.

[11] ZiyuanWang , "Security and privacy issues within the Cloud Computing" ,International Conference on Computational and Information Sciences , 2011

[12] ZaighamMahmood , " Data Location and Security Issues in Cloud Computing", International Conference on Emerging Intelligent Data and Web Technologies, 2011.

