IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 19, Issue 2, Ver. IV (Mar.-Apr. 2017), PP 67-72
www.iosrjournals.org

"Security Issues and Solutions in Cloud Computing".

Arun Kumar Sen[1], Pradeep Kumar Tiwari[2]
[1]*Dep. of Computer Science and Engineering Vindhya Institute of Technology & Science,Satna(MP)*
[2]*Dep. of Computer Science and Engineering Manipal University Jaipur*

***Abstract**: Cloud Computing provide a solution of computing problems. Cloud users can fulfill his/her need for all hardware, operating system and software applications by using the Cloud services. These features of cloud attract to people to use them. Cloud users mainly don't know about the vulnerabilities and threats before adopting the cloud services. This paper represents the brief knowledge of cloud services and cloud deployment models. In this paper, We attempt to describe the Security challenges in the application and data security at SaaS. This paper purpose is to provide a security perspective of SaaS service and how to resolve that problem in an easy way.*

***Keywords:** Cloud Security, Plate form as a Service, Infrastructure as a Service*

I. Introduction

New computing era, the concept of cloud computing become more popular because of his cost and elasticity. Cloud computing represent the combined model of distributed processing, parallel processing, and grid computing. Many companies like Google, Amazon AWS, IBM, Microsoft, Sun and much more are developing effective cloud computing technology and product [2]. Cloud computing, the long-held dream of "computing as a utility", has opened up the new era of future computing, transform a large part of IT industry, reshape the purchase and use of IT software and hardware, and receive considerable attention from global and local IT players, national governments, and international agencies [1].cloud computing provide three services and four deployment model. The services are respectively referred to as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) and deployment models are Private Cloud, Public Cloud, Hybrid Cloud and Community level Cloud. This paper aims to highlight the security issue and trust issue on using the SaaS. This paper will help to understand security issue and solution in current existing SaaS environment.

II. Cloud Computing

Cloud Computing is a technology which using the internet and central remote services in order to maintain data and application. A simple example of cloud computing is YAHOO or GMAIL user doesn't need software or a server to use them. The service is fully managed by the provider which means the user only needs a personal computer and Internet access [3].

NIST Definition-Cloud computing is a model for enabling 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 rapidly provisioned and released with minimal management effort or service provider interaction this cloud model is composed of five essential characteristics, three service models, and four deployment models [4].

2.1. Essential Characteristics:

According to the National Institute of Standards and Technologies (NIST), cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

This cloud model is composed of five essential characteristics:

On-demand self-service. Cloud services such as web applications, server time, processing power, storage, and networks can be provisioned automatically as needed by the consumers without requiring human interaction [19].

Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations)[4].

Resource pooling. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location-independence in that the customer generally has no control or

knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth [4].

Rapid elasticity. This is one of the key characteristics if your application experiences spike in usage. This does not need to be fully automated, but it should be relatively easy to provision additional servers if you have anticipated heavy usage. You may want to consider a base "plan" of servers and a payment model to handle spikes [20].

Measured Service (Pay-Per-Use) –Any resources that are used are carefully monitored, controlled and recorded which allows the cloud service provider to be completely transparent with the consumer of the resources and facilities. The user only pays for a number of resources they consume and are always made aware of any discrepancies, spikes or abnormal behavior regarding resources [21].

2.2. Service Models: Service delivery in Cloud Computing comprises three different service models, namely Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). The three service models or layer are completed by an end user layer that encapsulates the end user perspective on cloud services.

Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g.,web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings [4].

Platform as a service (PaaS). Platform-as-a-Service (PaaS) is a set of software and development tools hosted on the provider's servers. It is one layer above IaaS on the stack and abstracts away everything up to OS, middleware, etc. This offers an integrated set of developer environment that a developer can tap to build their applications without having any clue about what is going on underneath the service. It offers developers a service that provides a complete software development life cycle management, from planning to design to building applications to deployment to testing to maintenance. Everything else is abstracted away from the "view" of the developers. Platform as a service cloud layer works like IaaS but it provides an additional level of 'rented' functionality. Clients using PaaS services transfer even more costs from capital investment to operational expenses but must acknowledge the additional constraints and possibly some degree of lock-in posed by the additional functionality layers [17,18].

Infrastructure as a Service (IaaS). Infrastructure as a Service is a single tenant cloud layer where the Cloud computing vendor's dedicated resources are only shared with contracted clients at a pay-per-use fee. This greatly minimizes the need for huge initial investment in computing hardware such as servers, networking devices, and processing power. They also allow varying degrees of financial and functional flexibility not found in internal data centers or with co-location services, because computing resources can be added or released much more quickly and cost-effectively than in an internal data center or with a co-location service [14,16].

2.3. Deployment Models:

Cloud service can be deployed in different ways depending on the organizational structure and need of use. Cloud have mainly four deployment models Private cloud, Public cloud, Community cloud and Hybrid cloud.

Private Cloud. This model of Cloud computing is provided by an organization or its designated service provider and offers a single-tenant operating environment with all the benefits and functionality of elasticity and the accountability/utility model of Cloud computing. The physical infrastructure may be owned by and managed by the organization or the designated service provider with an extension of management and security control planes controlled by the organization[13].

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].

Public Cloud. A public cloud is a model which allows users' access to the cloud via interfaces using mainstream web browsers. It's typically based on a pay-per-use model, similar to a prepaid electricity metering system which is flexible enough to cater for spikes in demand for cloud optimization. This helps cloud clients to better match their IT expenditure at an operational level by decreasing its capital expenditure on IT infrastructure [14,15].

Hybrid Cloud. The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology, that enables data and application portability (e.g., cloud bursting for load-balancing between clouds)[22,23].

III. Securities Issues For Saas

The main question is how to solve security issue in cloud computing.Before solving the security problem firstly we can understand vulnerabilities, threats, and risk in cloud computing. The aim of this work that identifies the vulnerabilities and threats with the possible solution. The keywords and related concepts that make up this question and that were used during the review execution are- secure Cloud systems, Cloud security, delivery models security, SaaS security, PaaS security, IaaS security, Cloud threats, Cloud vulnerabilities, Cloud recommendations, best practices in Cloud.

Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g.,web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings [4].

IV. Security Issues In Saas

In Software as a Service (SaaS) model, the client has to depend on the service provider for proper security measures. The provider must ensure that the multiple users don't get to see each other's data. So, it becomes important to the user to ensure that right security measures are in place and also difficult to get an assurance that the application will be available when needed[6,7].

4.1. Privacy and Security in SaaS.

One of the best ways to assess a SaaS vendor's privacy and security measures is through the use of third-party certification procedures. Perhaps the most relevant certification, known as ISO 27001, is designed specifically to "provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an information security management system." This rigorous certification process focuses on a number of key requirements, including.

- The use of best practices to ensure the privacy, integrity, and availability of customer data.
- A provider's willingness to submit its data center and related operations to periodic certification audits [10]. Availability and disaster recovery are an important consideration when selecting a SaaS provider. Extended outages, downtime, or data loss can be costly and damage for a business.

4.1.1. Application Security

This guidance is for all stakeholders (including applications designer, security professionals, operations personnel and technical management) on how to best mitigate risk and management assurance when designing cloud computing application [12].

4.1.1.i. Extension to enterprise infrastructure.

- **Application Security Architecture –** Consideration must be given to the reality that most applications have dependencies on various other systems. With Cloud Computing, application dependencies can be highly dynamic, even to the point where each dependency represents a discrete third party service provider. Cloud characteristics make configuration management and ongoing provisioning significantly more complex than with traditional application deployment. The environment drives the need for architectural modifications to assure application security[5].
- **Secure Software Development Life Cycle (SSDLC)** –A Secure Software Development Life Cycle (SSDLC) (also referred by a few as secure development life cycle (SDLC) has assumed increased importance when migrating and deploying applications in the cloud.Organizations should ensure that the best practice of application security, identity management, and privacy are integral to their development program and throughout the lifecycle of the application [12].
- **Compliance –** Compliance clearly affects data, but it also influences applications (for example, regulating how a program implements a particular cryptographic function), platforms (perhaps by prescribing operating system controls and settings) and processes (such as reporting requirements for security incidents) [5].
- **Tools and Services –** Cloud computing introduces a number of new challenges around the tools and services required to build and maintain running applications. These include development and test tools, application management utilities, the coupling to external services, and dependencies on libraries and

operating system services, which may originate from cloud providers. Understanding the ramifications of who provides, owns, operates, and assumes responsibility for each of these is fundamental[5].

- **Vulnerabilities –** These include not only the well-documented—and continuously evolving—vulnerabilities associated with web apps, but also vulnerabilities associated with machine-to-machine Service-Oriented Architecture (SOA) applications, which are increasingly being deployed into the cloud [5]

4.2.1. Data Security

Cloud computing needs to process and analyze mass and distributed data, therefore, data management technology must be able to efficiently manage large data sets[27].Enterprise data need protection and the accountability lies with the SaaS vendor. The aspect of data integrity should be ensured by the SaaS Vendor which signifies the fact that data of each enterprise tenant should not be available for another client throughput the life cycle of data [24].

Before adopting the SaaS service some important question keeps in your mind related to data Security.

1. How do you protect user authentication information?
2. How are User Files stored? What level of encryption?
3. Is the system multi-tenant?
4. How is account information stored?
5. Are User Files accessed by the vendor?
6. Who has access to User Files?
7. When are files deleted?
8. How is disk media destroyed when decommissioned?
9. How data is transferred (both account information and User Files)?
10. Is data backed up or copied [11]?

The answer to all these questions should be found by application users. Saas service provider ensures authentication and validation of users. Check user's identity before accessing the user's data. It means when the users want to access the data, that time check users name, password and security question answer. SaaS service provider always must be serious about customer data theft by encryption method.

Many times same application open for different users.Users are accessing the same application that time users save , update or delete the data with the help of same application. SaaS provider ensures that all the data separately stores and sensitive (important) data store with more security features. Occasionally user's loss or delete the data accidently that time it gives the backup and recovery to users of his loss data. Sometimes users required backup or copy of the data, service provider provide the backup features to users and also ensure the high security of this data.

Users have multiple options to use application using service, for example, user can use the application in desktop, laptop or mobile. SaaS provider provides the application in all application access equipment with portability.

In SaaS, organizational data is often processed in plain text and stored in the cloud. The SaaS provider is the one responsible for the security of the data while is being processed and stored[8,9] In the world of SaaS, the process of compliance is complex because data is located in the provider's data centers, which may introduce regulatory compliance issues such as data privacy, segregation, and security, that must be enforced by the provider [8].

The organizations using cloud computing should maintain their own data backups even if the providers backs up data for the organization. This will help continuous access to their data even at the extreme situations such as data providers going bankruptcy or disaster at data center etc[28].

When the user's data are shared among different servers that time service provider must ensure to the user his account is highly secure and he is the only person who can access his data. The service provider also ensures that his important data in on backup mode and he can recover his data anytime. Provider ensures to the user server crash won't create a problem.Provider provides user data from another server.

4.2.2.i. Encryption and data Protection

Several solutions have been proposed for the security and privacy problem. The most obvious way out for users is to encrypt whatever data they are going to put in the cloud. Cryptography is a widely used technique which is reliable for data security. But it will increase the cost of computation and it is technically cumbersome to process the data in an encrypted form [25]. To guarantee the privacy of information hosted on servers in the cloud, the information could be encrypted which can only be decrypted at the client level with a key. Again this is only reliable if the data can be quickly decrypted at the client level as it might need high processing power. The multi-core processors which are evolving will make this possible and provide greater integration of information [28]. The data is to be encrypted and compressed in multi-server. In encryption and compression, the data that has to stored in a cloud cannot be stored in a text format due to security reasons so it must be

transformed into an encrypted format. The data also has to be compressed for secure transmission. This method deals with the compression and encrypts the data before it is taken as a back up in multi-server [29]. Using a combination of asymmetric and symmetric cryptographic (often referred to as hybrid cryptography) can offer the efficiency of symmetric cryptography while maintaining the security of asymmetric cryptography [22].
The protection of information privacy: government committee for developing the security standard technology and notification of information security breach. As a matter of fact, a lot of states in the United States have enacted the law for notification of security breach for computerized personal information [25,26].
Even though the United States is trying to enforce the protection of information privacy, especially within cyberspace, there is one commonly criticized problem hidden in "The Stored Communications Act", which is codified in chapter 121 from section 2701 to 2712 in U.S. Code [25].

Some widely known cryptosystems include RSA encryption, Schnorr signature, El-Gamal encryption, PGP, More complex cryptosystems include electronic cash systems, encryption systems, Some more theoretical cryptosystems include interactive proof systems, (like zero-knowledge proofs), systems for secret sharing etc.

Many analysis experts find the conclusion cryptography also have some weakness and insecurity under the cryptographic scheme. Encryption method can be broken by a hacker after some or many efforts. Security of message also depends on the size of key and method which are used for encryption. Highly encrypted data can be secure from forgery. Cryptography is the best method to secure data.

V. Conclusion

Cloud computing is a new and promising paradigm to delivering the IT services as computing utilities. Clouds are designed to provide services to external users; providers need to be compensated for sharing their resources and capabilities. In this paper, we discussed the problem of security, need of security and what the approaches are needed for application and data security. We have to approach implementing and enforce security issue in SaaS service. The transparency of access data and application use should be authentic with security mechanism. A lot of work already done in the field of security but still, now some security protection already need. In this paper, we are trying to understand what is a cloud? Why cloud? Services of cloud, models of cloud, characteristics of cloud and security in SaaS (application security and data security).This paper will helpful for understanding cloud and SaaS security.

References

[1]. Sun Dawei, Chang Guerin , Sun Lina and Wang Xingwei, Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments Published by Elsevier Ltd,Procedia Engineering 15(2011).
[2]. Liu Kun, Dong Long-Jiang, Research on Cloud Data Storage Technology and Its Architecture Implementation, 2011 Published by Elsevier Ltd. 2012 International Workshop on Information and Electronics Engineering (IWIEE).
[3]. Fauzi the Annual Azila ,Herawan Tutut, Noraziah A. ,Noriyani Mohd .Zin , On Cloud Computing Security Issue, Springer-Verlag Berlin Hiedelberg 2012.
[4]. Mell Peter , Grance Timothy , The NIST Definition of Cloud Computing , NIST Special Publication 800-145 .
[5]. Cloud Security Alliance , Security Guidance for Critical Areas of Focus in Cloud Computing V2.1 , Cloud Security Alliance December 2009.
[6]. Rashmi, Dr Sahoo G., Dr. Mehfuz S., 1Securing Software as a Service Model of Cloud Computing: Issues and Solutions , International Journal on Cloud Computing: Services and Architecture (IJCCSA) ,Vol.3, No.4, August 2013.
[7]. Choudhary V.(2007). Software as a service: implications for investment in software development. In:International conference on system sciences, 2007, p. 209.
Hashizume Keiko , Rosado G David , Fernández-Medina Eduardo and Fernandez B Eduardo, An analysis of security issues for cloud computing , Journal of Internet Services and Applications2013,4:5,http://www.jisajournal.com/content/4/1/5.
[8]. Ju J, Wang Y, Fu J, Wu J, Lin Z (2010) Research on Key Technology in SaaS.In: international Conference on Intelligent Computing and Cognitive Informatics (ICICCI), Hangzhou, China. IEEE Computer Society, Washington,DC, USA, pp 384–387.
[9]. A Websense White PaperSeven ,Criteria for Evaluating Security-as-a-Service (SaaS) Solutions, http://www.websense.com/assets/white-papers/whitepaper-seven-criteria-for-evaluation-security-as-a-service-solutions-en.pdf.
[10]. SaaS Security Assessment Guide , https://www.hightail.com/en_US/docs/HT_Security_WhitePaper.pdf
[11]. Cloud Security Alliance ,Security Guidance for Critical Areas of Focus in Cloud Computing V3.0 , Cloud Security Alliance 2011.
[12]. Modelling Cloud Computing Architecture Without Compromising Privacy , Information and Privacy Commissioner,Ontario, Canada May 2010.
[13]. Ramgovind S, Eloff MM, Smith E , The Management of Security in Cloud Computing , 978-1-4244-5495-2/10, IEEE 2010.
[14]. A Platform Computing Whitepaper, 'Enterprise Cloud Computing:Transforming IT', Platform Computing, pp6, viewed 13, March 2010.
[15]. Brodkin J, 2008, 'Gartner: Seven cloud-computing security risks', Infoworld, viewed 13 March 2009, from http: / /www.infoworld .com /d/security-central/gartner-seven-cloud-computing-security-risks-853?page=0,1.
[16]. Kuyoro S. O., Ibikunle F. , Awodele O., Cloud Computing Security Issues and Challenges , International Journal of Computer Networks (IJCN), Volume (3) : Issue (5) : 2011.
[17]. Global Netoptex Incorporated. "Demystifying the cloud. Important opportunities, crucial choices." pp4-14. Available: http://www.gni.com [Dec. 13, 2009].
[18]. Ahmed E. Youssef, Exploring Cloud Computing Services and Applications, Journal of Emerging Trends in Computing and Information Sciences, VOL. 3, NO. 6, July 2012.
[19]. Olive Christopher, Cloud Computing Characteristics Are Key, White Paper, General Physics Corporation 2011.

[20]. Carlin Sean, Curran Kevin , International Journal of Cloud Computing and Services Science (IJ-CLOSER) Vol.1, No.2, June 2012, pp. 59~65 ISSN: 2089-3337 .
[21]. Zissis Dimitrios , Lekkas Dimitrios , Addressing cloud computing security issues , Elsevier journal Future Generation Computer Systems 28 (2012) 583–592 .
[22]. National Institute of Standards and Technology, The NIST Definition of Cloud Computing, Information Technology Laboratory, 2009.
[23]. Vemulapati Jyanti,Neha Mehlotra and Dangwal Nitin ,SaaS Security Testing: Guidelines and evaluation framework ,11th annual International Software testing conference 2011.
[24]. Tiwari, P. K., & Joshi, S. (2014, December). A review of data security and privacy issues over SaaS. In Computational Intelligence and Computing Research (ICCIC), 2014 IEEE International Conference on (pp. 1-6). IEEE..
[25]. Sotto LJ, Treacy BC, McLellan ML. Privacy and data security risks in cloud computing. Electronic Commerce & Law Report2010, 15 ECLR 186.
[26]. Tiwari, P. K., & Joshi, S. (2016). Data security for software as a service. In Web-Based Services: Concepts, Methodologies, Tools, and Applications (pp. 864-880). IGI Global.
[27]. Rajasekar Narendran Calluru , Security Implications Of Cloud Computing, MSC Internet Systems Engineering ,University of East London, November 30th, 2009.
[28]. Sajithabanu S.,Dr Prakash Raj. George E., Data Storage Security in Cloud, InternatIonal Journal of Computer ScienCe and technology, Vol. 2, Issue 4, Oct. - Dec. 2011.