IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

A Review on Security Issues and their Impact on Cloud Computing Environment

Sadhana Malgey[1], Mr. Pranay Chauhan [2]

M.Tech Scholar, Department of Computer Science & Engineering, SVCE, Indore, India [1]

Assistant Professor, Department of Computer Science & Engineering, SVCE, Indore, India [2]

Abstract: The cloud computing is a technology used to organize and manage resources and services. Cloud based Web applications help for enabling convenient and on demand resource access with resource shared pool. Cloud Computing application provides platform for various computation, software access and data handling for betterment of proposed solution. Security is primary requirement to maintain trust and authenticity of information and services. This research work observes that there is big gap into security issue of existing system. Confidentiality, authentication, access control and integrity are the major ideology of security and one of the essential requirements for any software. This paper investigate existing solution for SaaS model of Cloud computing and explore the various flaw in context of security. Here, work concludes with the comparative study of different existing solution and address the common problems and excuses.

Keywords: Cloud Computing, Security Issues, Hybrid Cloud, Security Techniques.

I. INTRODUCTION

Cloud computing is a new technology which is a result of wrapping Virtualization, parallel computing and distributed computing into a single unit. The NIST definition of cloud computing "Cloud computing is a delivery model that enabling ubiquitous, convenient, efficient on -demand network access to a pool of shared configurable computing resources such as networks, storage, applications, server and services that can be rapidly provisioned and reduced". This cloud model is consists of five essential characteristics, three service models and four deployment models.

The cloud computing is a web based model which is connected with more than one system. Cloud computing is the combination of fundamental technique which are utility computing and service oriented architecture.
Cloud computing means to deliver everything software and hardware by using internet. It removes the necessity of setting high cost devices for infrastructure for any organization, with the help of cloud computing the organization takes care of its functions work rather than to develop a costly infrastructure.

In cloud environment all the data are outsourced to external provider and they take concern of that data is now a responsibility of the cloud provider and we can access this data on virtual machines or any other device. Since the data center of cloud provider is spread to all over in the world and we can access our data from any corner of the world. Cloud Computing is the result of advancement in the presented technologies. At the current world of networking system, Cloud computing is one of the most important and developing idea for both the developers and the users. In the cloud environment, resources are shared among the servers, users and individuals.

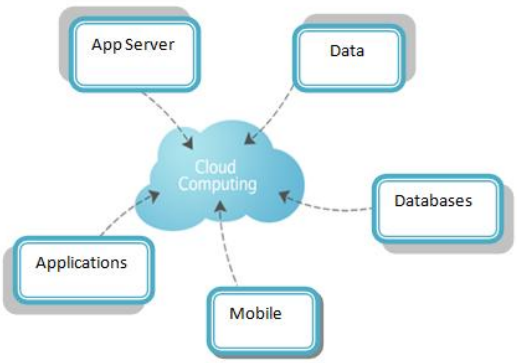

Figure 1.1: Cloud Computing

These Cloud services can be further comes under the three categories.

- SaaS- Application that is deployed over a network, typically the web, accessible via a browser or program interface; referred to as software on demand.
- PaaS- A platform on which user can build their application using languages, libraries, tools and services supported by provider.
- IaaS- Processing and storage capacity, networking and computing resources where the user has control over operating system and deployed application; sometimes referred to as utility computing.

Cloud Computing Deployment Models: cloud services are typically made available to its customer via a private, public, community, hybrid cloud.
Private Cloud- It is owned, maintained and used by a single organization and the services are used by their internal users. Users within the organization can use the data, available services and other application.

Copyright to IJARCCE
DOI 10.17148/IJARCCE.2016.5653

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

Public Cloud: It is owned and maintained by a single organization, but its services and application are available for general public use. In this all services are available and any user can get those services by paying appropriate amount.
Community Cloud: It is owned and maintained by an organization for a specific community. This cloud could be shared by many organizations for any particular reason; possibly it managed by internally or externally.
Hybrid Cloud - This type of cloud is a combination of two or more clouds (for example combining public and community clouds).

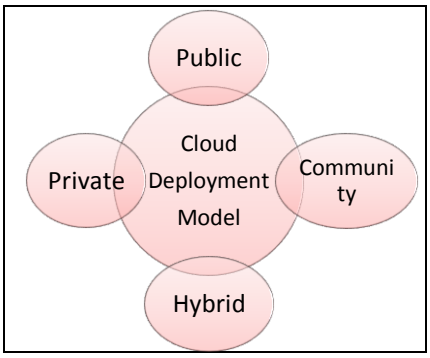

Figure 1.2: Cloud Computing Deployment Model.

Common Characteristics of Cloud Computing:
Cloud computing is based on five essential attributes: multi-tenancy (shared resources), massive scalability, rapid elasticity, and self-provisioning of resources; It make new advances in processors, Virtualization technology, disk storage and fast, inexpensive servers combined to make the cloud a more compelling solution.
The most important attributes of cloud computing is illustrated as follows:

- Multi-tenancy or shared resources: Cloud computing is based on business model in which resources are shared (i.e., same resource uses by the multiple users) at the network level, host level, application level.
- Massive scalability: Cloud computing provides ability to scale to tens of thousands of systems and as well as the ability to massively scale bandwidth and storage space.
- Elasticity: User can rapidly increase and decrease computing resources as needed.
- Pay as you used: Users to pay for only the resources they actually use and for only the time they need them.
- Self-provisioning of resources: Users self provision resources, such as added systems (i.e processing capability, software and storage) and network resources.

II. RELATED WORK

Security in cloud is one of the major areas of research. Many researchers have investigated on cloud security. Chen, D. et al. [4] address that data security affect a lot on the performance of cloud services. They do not help to maintain privacy and originality of content but also help to maintain trust and reliability on service as well service provider. The provide privacy protection mechanism concise all round analysis. They compare their solution with airawet and their concern is to avoid information leakage from cloud environment. They uses MapReduce framework for deployment of proposed solution.
Tumpe Moyo et al [5] discusses the different types of cloud computing technology and discusses about open source cloud is quickly developing and provides some benefit over proprietary, but currently the proprietary method appears to be best route to take due its stability. Security is still an issue within cloud computing but the research indicates that this is taking a positive turn and is greatly improving as the cloud technology and adoption develops. The survey results demonstrate the popularity of cloud technology. The survey findings will inform the development and deployment of a Cloud based e-learning tool with the required security features.
Dimitrios Zissis et al. [6] introducing a Trusted Third Party, tasked with assuring specific security characteristics within a cloud environment. This paper evaluates cloud security by identify security requirements and attempt to present a possible solution that eliminates these potential threats. In this paper identified generic design principles of a cloud environment which stem from the requirement to control relevant vulnerabilities and threats. A combination of PKI, LDAP and SSO can concentrate on most of the identified threats in cloud computing dealing with the integrity, confidentiality, authenticity and availability of the data and communications .Security requires a systemic point of view, from which security will be constructed on trust and mitigating protection to a trusted third party in a cloud computing environment.

K. Nasrin, et. al. [7] address that cloud storage frameworks are one of the key research area for cloud computing. Security is one of the major important concerns for research work. They derived a mechanism which is the combination of asymmetric and symmetric key method using RSA and AES algorithm. AES is good for key sharing and low overhead cryptographic mechanism further, RSA is good to create complex phenomena for attackers. The focus of the attackers was on proving secure file communication from vulnerable network. Jayant, D. et al. [8] proposed role base access control mechanism using AES and RSA algorithm to provide a secure environment for public cloud environment. Here, they uses RSA and AES model for encryption and decryption purpose where RBAC is used for access control purpose. It gives the uploading rights and different rights to different user as per RBAC model. Cindhamani.J et. al. [9] proposed an improved design for data security. It proposed a concept to achieve integrity, confidentiality and authentication in single architecture. They uses 128 bit key for RSA and Third party auditor for authentication purpose. Here, proposed solution consist two main parts one is storing data into storage and another is retrieve data from storage. This paper ensures the security goals during storage operations and guaranty about valid authentication and access. Kawser Wazed Nafi et al [10] also introduced a

improved framework for security similar with above researchers. They have also proposed OTP mechanism and security services for secure communication.

Mrudula Sarvabhatla et al. [11] introduced an improved mutual authentication scheme, which is secure and opposed to all major cryptographic attacks. proposed authentication scheme avoids the expensive resource consuming operations. With negligible computational overload on client and server side and ability to resists all major cryptographic attacks makes our scheme more practical and can be deployed in resource less environment. This scheme is mainly built upon less expensive operations like one-way hash computations and negligible resource consuming XOR operations. Improved mutual authentication scheme is divided into three stages: Registration stage, Login stage, Mutual authentication stage. Hussain Aljafer et al.[12] describe about some of the major approaches for secure data sharing in cloud computing environment and Specifically focus on the use of encryption schemes and also provide a comparative study of the major schemes, through implementation of some representative frameworks. The survey is to show how encryption is used in every of the covered technique, and discusses the corresponding open issues The objective is to provide a concise survey of existing solutions, discuss their benefits, and point out any shortcomings for future research.

Following major problems has been observed during the study. In the table below a comparative study about security issues in cloud computing:

TABLE I Comparative Study

S. No	Title	Author	Research	Year	Problem Domain
1.	Investigating Security Issues in Cloud Computing	Tumpe Moyo, Jagdev Bhogal	Discusses the different types of cloud computing technology and discusses about open source cloud is quickly developing and provides some benefit over proprietary.	2014	Cloud security issues
2.	Data Security and Privacy Protection Issues in Cloud Computing	Deyan Chen, Hong Zhao	The provide privacy protection mechanism concise all round analysis. They compare their solution with airawet and their concern is to avoid information leakage from cloud environment.	2012	Data security and privacy protection issues exist in all levels in SPI service models
3.	Addressing cloud computing security issues	D. Zissis, D. Lekkas	Addresses cloud security by identify unique security requirements and to attempt to present a feasible solution that eliminates potential threats. Introducing a Trusted Third Party.	2012	a number of unchartered risks and challenges
4.	A Framework Based on RSA and AES Encryption Algorithms for Cloud Computing Services	Nasrin Khanezaei, Zurina Mohd Hanapi	Based on combination of RSA and AES Encryption methods, provide difficulty for attackers as well as reducing the transmission time of information.	2014	Loss of control over, data and the risk of accessing data by attackers.
5.	Private Cloud Security: Secured user Authentication by using Enhanced Hybrid Algorithm	Nikhil Gajra, Shamsuddin S. Khan, pradnya Rane	Hybrid of AES and Blowfish for encryption, provide security guarantees not only on authentication but also on files over the cloud for the outsourced data.	2014	Human level risk, unauthorized access on files.
6.	A Robust Mutual Authentication Scheme for Data Security in Cloud Architecture	Mrudula Sarvabhatla, Chandra Sekhar Vorugunti	Propose an improved mutual authentication scheme, which is secure and resistant to all major cryptographic attacks.	2015	Security issues like User authentication, integrity of data etc. And cryptographic attacks.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

7.	An enhanced data security and trust management enabled framework for cloud computing systems	Cindhamani, Naguboynia Punya, Rasha Ealaruvi, L.D. Dhinesh babu	Data protection by using the algorithms such as 128 bit encryption algorithm And RSA algorithm, follows the security polices such as Integrity, confidentiality and availability.	2014	Data security in cloud.

III. PROBLEM STATEMENT

The security issues in cloud computing includes:

- Data security
- Identity and access control
- Key management
- Virtual machine security

Among these main security issues in the cloud, data security and integrity is believed to be the most difficult problem which could limit the use of cloud computing. In fact, access control and key management are all issues involved in data security. Data security in the cloud refers to data confidentiality, integrity, availability and traceability (CIAT), and these requirements pose major problems for cloud computing.

Confidentiality: Data confidentiality requires that information be available or disclosed only to authorized individuals, entities or IT processes.

Integrity: Data integrity ensures that the data is maintained in its original state and has not been intentionally or accidentally altered or deleted.

Availability: Data availability ensures continuous access to data even in the occurrence of a natural or man-made disaster or events such as fires or power outages.

Traceability: Data traceability means that the data and communications are genuine in a transaction and that both parties involved are who they claim to be.

Authentication: Authentication is a method by which a system verifies and validates the identity of a user of the system who wishes to access it.

Specifically, to achieve the above requirements of CIAT, the critical security challenges of data security in the cloud can be mainly outlined as follows:

1. Key management
2. Access control
3. Searchable encryption techniques
4. Remote integrity check
5. Proof of ownership

Understanding of security threats in hybrid cloud computing environment to propose authentication system suitable for hybrid cloud services is required. So we will divide and describe five kinds of threats that as follows.

1. Man-in-the-middle attack or man-in-the middle-browser attack. This threat arise between authentication server on internal network and outside user such as smart phone, tablet.
2. DoS or DDoS attack.
3. Third threat is location certification attack. On the outside, mobile devices move very frequently but mobile device's location information is important for its certification.
4. Fourth threat is script attack weakness by inside attacker.
5. Outside user authentication for public cloud service.

TABLE III Security Threats in Cloud Environment

Attack	Description
Tampering	An attacker may alter or fabricate information.
Eavesdropping Information Disclosure	Attacker may listen or read the information.
Repudiation	Attacker may refuse the validity or claim of information or service.
Man-in-the-Middle Attack	Attacker may intercept the communication and deploy third party involvement.
Replay Attack	Attacker may hold and resend the packet information after a time delay.
Identity Spoofing	Attacker may destroy or misuse the identity of node, server or client.
Viruses and Worms	Attacker may use certain bad source code to compromise.

IV. CONCLUSION

Cloud computing is the new paradigm where computing is on demand service. When company decides towards to cloud computing, it loses control over the data. So providing security of its data during transmission and that is stored into the cloud is the major problem. Any application relying upon an emerging technology should consider the different possible threats. The various security issues presented in this paper would definitely benefit the cloud users to suggest proper choice and cloud service providers to handle such threats efficiently. Thus, in our survey paper, a study of cloud security environment and requirement of cloud security has been explored and address with problem observations. As on now cloud is changing the way a user works over the network. It continuously reduces the load on users in terms of cost and complexity. It also lets the organization feel safe about their data against security breaches and fault interruptions. It provides a robust way of serving user through a service based model.

Copyright to IJARCCE
DOI 10.17148/IJARCCE.2016.5653

REFERENCES

[1] Daryl C. Plummer, Thomas J. Bittman, Tom Austin, David W. Cearley, David Mitchell Smith, "Cloud Computing: Defining and Describing an Emerging Phenomenon", in Research at Gartner Publication, ID Number: G00156220, 2008.
[2] http://www.cloudsecurityalliance.org.
[3] "Security Breaches-Challenges and Solutions", White Paper at CA Technologies Security Management, 2012.
[4] Deyan Chen and Hong Zhao "Data Security and Privacy Protection Issues in Cloud Computing" 2012 IEEE International Conference on Computer Science and Electronics Engineering.
[5] Tumpe Moyo, Jagdev Bhogal "Investigating Security Issues in Cloud Computing" 2014 IEEE Eighth International Conference on Complex, Intelligent and Software Intensive Systems.
[6] Dimitrios Zissis, Dimitrios Lekkas "Addressing cloud computing security issues" Future Generation Computer System Volume 28, Issue 3, March 2012, (583–592) , Elesvior.
[7] Nasrin Khanezaei, Zurina Mohd Hanapi "A Framework Based on RSA and AES Encryption Algorithms for Cloud Computing Services" IEEE Conference on Systems, Process and Control (ICSPC 2014), 12 - 14 December 2014, Kuala Lumpur, Malaysia.
[8] Bokefode Jayant D, Ubale Swapnaja A, Pingale Subhash V, Karande Kailash J., Apate Sulabha S., "Developing Secure Cloud Storage System by Applying AES and RSA Cryptography Algorithms with Role based Access Control Model" International Journal of Computer Applications (0975 – 8887) Volume 118– No.12, May 2015.
[9] Cindhamani.J, Naguboynia Punya, Rasha Ealaruvi, L.D. Dhinesh babu "An enhanced data security and trust management enabled framework for cloud computing systems" IEEE 5th International Conference on Computing, Communications and Networking Technologies July 11-13, 2014, Hefei, China.
[10] Kawser Wazed Nafi, Tonny Shekha Kar, Sayed Anisul Hoque, Dr. M. M. A Hashem "A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing security architecture" (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No. 10, 2012.
[11] Mrudula Sarvabhatla, Chandra Sekhar Vorugunti "A Robust Mutual Authentication Scheme for Data Security in Cloud Architecture" IEEE Future Information Security Workshop, COMSNETS 2015.
[12] Hussain Aljafer, Zaki Malik, Mohammed Alodib, Abdelmounaam Rezgui "A brief overview and an experimental evaluation of data confidentiality measures on the cloud" journal of innovation in digital ecosystems 1 (2014) 1 – 11, Elesvior.
[13] Nikhil Gajra, Shamsuddin S. Khan, pradnya Rane "Private Cloud Security: Secured User Authentication by using Enhanced Hybrid Algorithm" IEEE 2014 International Conference on Advances in Communication and Computing Technologies.

DOI 10.17148/IJARCCE.2016.5653