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 Study of Security Requirements in Cloud Computing Environment

Naziya Khan[1], Mrs. Asha Khilrani[2]

M.Tech. Scholar, Department of Computer Science & Engineering, T.I.T. & Science, Bhopal, India [1]

Assistant Professor, Department of Computer Science & Engineering, T.I.T. & Science, Bhopal, India [2]

Abstract: Cloud computing is a technology helps to share resource, services and platform with another user. This is a technology used to organized huge amount of data and multiple services for establishing convenient way of communication and execution. In simple words, cloud computing technology help to access services and resource without installing or configuring into local system. Cloud computing establish their access through public network, security issues like privacy, trust, authenticity , information security, authorization, access control becomes essential challenges for developers. In order to overcome these challenges, various algorithms are developed and implemented with cloud computing applications to get best way for implementation. Today, security becomes indispensable concern and required separate attention for cloud computing environment. This research works consider this issue on primary mode and try exploring algorithms and their limitations to observe and analyse security solutions and vulnerabilities for scope of improvement. 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 technology is seen as the collection of internet based services for better utilizing the resources and services. It is the new utility which provides virtualization, parallel and distributed computing into single unit. It implies the sharing of resources to handle applications with reduces capital and cheaper maintenance cost. It gives increased scalability and ease of access feature with low complexity.

Cloud computing can be defined as It is a model that offers its Client; on-Demand network access to a shared pool of resources such that networks, storage, applications server and services, that can be rapidly provisioned and released with minimal management effort. The cloud model consists of five vital characteristics and three service model. Cloud computing is technology which is not product but more than service provision. It is the combination of computing and services. It believes in anything –anywhere concept and provides services through internet at single browser.

Five essential component of cloud environment can be listed below;

1. Data: It the collection of raw material which may be useful may not.
2. Storage: This is the organized set of information for easy access, update and management purpose. It considers datacenters, disk, taps for storage purpose and database servers for organization of data.
3. Client Networks: It includes various devices like PDA, Smart Phone, I-Phone, Computers, laptops etc. It may classified as mobile client, think and thick client.
4. Applications & Computing:

Applications are the human or machine developed computing program helps to fulfill the requirement and execution of task. Further, it requires Computing, which is the goal of oriented activity creating sequence of steps using algorithms.

5. Virtualization:

It is the creation of virtual version rather than actual. It helps to access resources and services. A block representation of component architecture of cloud computing is shown in figure 1.

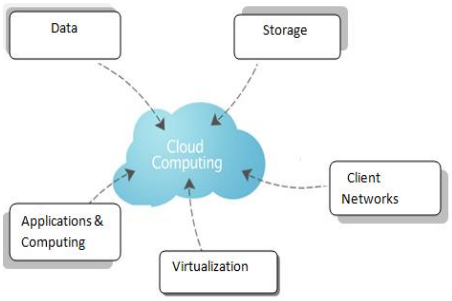

Figure 1: Components of Cloud Computing

The cloud computing environment always implemented with the help of cloud services. It can be described as follows.

1. Software as a Service [SaaS]:

This service configures access of software and application our networks. It can be accessed through browser of referred to as software on demand facility.

2. Platform as a Service [PaaS]:

A collection of libraries, runtime environment, development languages, and system software may know as the platform. This service helps to access platforms and execution environment using internet services.

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

3. Infrastructure as a Service [IaaS]:
Infrastructure may consider as the storage or processing capability of the node. IaaS provides facility to share resources and deployed application as utility computing.
Cloud Computing Deployment Models: cloud services are very typically made available to its customer via types of cloud. A brief review of types of cloud is cited below.
Private Cloud: It delimits the services deployment and access up-to limited network are. It is owned, maintained and accessed by single organization and deployed within intranet. Users within the organization can use the data, available services and other application.
Public Cloud: This type of cloud required implementation of cloud services using internet facility. It may own by single user but provides facility for general public also. 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, in terms of cost it is cheaper than private but costlier than public.
Hybrid Cloud - This type of cloud is a combination of two or more clouds (for example combining public and community clouds).

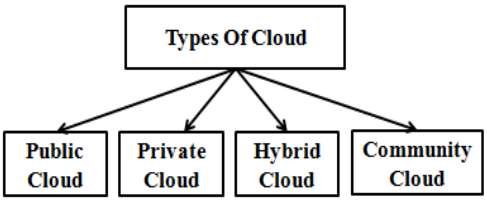

Figure 2: Cloud Computing Service model.

II. RELATED WORK

Chen, D.[1] et. al. address that information security affect the performance of cloud applications and may degrade the quality of service execution. Opponent may explore the vulnerabilities and deploy security threats or sniffing activity to compromise the privacy of the communication. So, to maintain the user trust and reliability on services as well improvement into quality of services execution, a implementation of security model is mandatory. Finally, they compare their solution with airawet framework and try to reduce information leakage issue. Tumpe moyo et. Al. [2] discusses the different types of cloud computing technology and discusses the results of this research survey which was proposed to test the obstruction protecting organizations from adopting cloud (with a particular focus on the security issues).The survey respondents mainly preferred the use of hybrid or private cloud. The survey results show the popularity of cloud technology. security is still an issue within cloud computing but the above research indicates that this is taking a positive turn and is greatly improving as the cloud technology and adoption develops. Kai Hwang et. Al.[3] illustrates Data coloring and software watermarking techniques prevents shared data objects and Broad distributed software modules. These techniques precautions multi-way authentications, enable single sign-on in the cloud and tighten access control for sensitive information in public and private clouds .By Implementing this idea cloud providers can implement the data-coloring mechanism ,proposed reputation system to secure data center access at a crude-grained level ,secure data access at a fine-grained file level. Nasrin Khanezaei, et. al. [4] explores that cloud frameworks is one of the major utility phenomena for today's development. Here, they explores the recent issues and address security as the one of the major concern for cloud computing. Assurance about security services not only helps to maintain privacy and originality of information but maintain user trust on service providers. To implement the security mechanism with cloud environment they uses AES and RSA algorithm with key sharing mechanism. AES is a symmetric key algorithms used to generate private key for RSA algorithms. Furthermore, RSA supports variable key length with strong cryptographic algorithm. Finally, they only focus on secure file communication and succeed to achieve confidentiality with cloud applications. Cindhamani.J et. al. [5] address that there is strong need to revised the data security design and add security as the integrated component of cloud environment. They uses a 128-bit key for RSA algorithm and third party auditor to keep safe eye of authentication and verification process.
Here, deployed solution improves the security feature into two ways one is storage end and another is access of information. Pin Zhang et. Al.[6] focused on the security control intensity at real- time congestion level of the system. With the control of various security strength, the same role had different activated permits. They solved the problem of the protecting the privacy of users' permissions. the algorithm had similarities in the sensitive degree of malicious attacks and penalties. When malicious user attacking, the user's trusted level and trusted value would be difficult to return to the previous level, thus they think to resist malicious attacks. They maintained other factors stable and changed only a factor, the sensitive degree of malicious attacks and penalties would be eased, and the sensitivity and penalties would change with the change of the importance degree of various factors. Nikhil Gajra et. Al. [7] describes a new mechanism, the hybrid of blowfish and AES for encryption of data.ECC is used for key generation and DH is applied for key agreement. The combination of these techniques for key management is known as ECDH (Elliptic curve Diffie-Hellman) Key Exchange.This research provides better security for outsourced data.by mixing DH and ECC it provides high security and takes small time for encryption. Mahnoush Babaeizadeh et. Al.[8] mainely focuses on Authentication methods in CC. Authentication is an important issue in CC ,it is preserving security and privacy for each communication in CC. By using a safe authentication mechanism a client can preserve his critical and sensitive information in CSP. Authentication determines the valid user in CC. There are many methods for authentication such as MTM, PKI ,user name–Password Scheme , Biomatric Authentiaction etc.B.Sumitra et. Al. [9] focused

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

on identifying the various authentication attacks in CC environment. An attempt has been made to understand the root cause of the authentication attacks and proposed possible mitigation measures in a cloud environment. strong user authentication mechanisms restricting illegal access are the primary requirement for securing cloud. A user authentication mechanism designed for cloud should be strong enough to protect cloud from different possible authentication attacks. This paper surveys the authentication attacks on cloud and the corresponding mitigation measures. Computer Forensics Community [10] represents collision in MD5 Algorithm. A collision effect is when we find two files to have the same hash. The research published by Wang, Feng, Lai and Yu illustrated that MD5 fails this third requirement since they were be able to give two different messages that have the same hash. This research gives mathematical information that how to design hash functions to improve the next generation's codes.

Following key problems has been observed during the study in Table I:

TABLE I Comparative Study

S. NO	Title	Author	Year	Problem	Technique Used	Research
1.	Three step data security model for cloud computing based on RSA & Stegnography techniques.	Vinay kumar pant et. Al.	2015	Security of stored data & Information in CC.	RSA Algorithm & Stegnography.	Proposed three step data security model to secure cloud data. They used RSA for encryption and decryption, steganography technique for hide data within the image.
2.	Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing	Mr. Prashant Rewagad et. Al.	2013	security concerns like privacy, data security, confidentiality, and authentication	Digital signature and DH key exchange blended with AES	DH algorithm is used to generate keys for key exchange. Then digital signature is used for authentication, there after AES is used to encrypt or decrypt user's data file.
3.	An enhanced data security and trust management enabled framework for Cloud computing systems	Cindhamani et. Al.	2014	Secured data protection.	128 bit RSA algorithm.	Assures security aspects such as integrity and authentication to make storage of data highly secured. User's identification by digital signature that performs the authentication process.
4.	Enhancing the Data Security in Cloud by Implementing Hybrid (Rsa & Aes) Encryption Algorithm	Vishwanath S Mahalle et. Al.	2014	Secure Upload and Secure Download of data in Cloud.	RSA and AES algorithms.	RSA and AES encryption algorithm offers three keys for encryption and decryption. Data stored in encrypted form , only decrypted by the secret key and private key of the user.
5.	Private Cloud Security: Secured on by using Enhanced Algorithm	Nikhil Gajra et. Al.	2014	Authentication and security on files over the cloud.	Elliptic Curve Diffie Hellman (ECDH), Modified AES	AES and Blowfish are used for encryption and have a impact on authentiction.ECC and DH takes small time for encryption and provide good security in CC.
6.	A Novel Cryptographic and Steganographic Approach for Secure Cloud Data Migration	Ankit Dhamija et. Al.	2015	Secure transfer of data from cloud servers is important.	Symmetric key Cryptography and Steganography(LSB Method)	Symmetric cryptographic technique is used to generate dynamic value for the private Key that makes it very Safe.in second step they used LSB method for stegnography.
7.	Secured User's Authentication and Private Data Storage- Access Scheme in Cloud Computing Using Elliptic Curve Cryptography	Shilpi Singh et. Al.	2015	User's authentication, data leakage and loss of data are the important security issues in CC.	ECC, ECDH, OTP	ECC and ECDH are applied to provide same level of security with minimal key size. user will securely validated itself by using variant input parameters at the time of login to the cloud server.

DOI 10.17148/IJARCCE.2016.5654

8.	A Framework Based on RSA and AES Encryption Algorithms for Cloud Computing Services	Nasrin Khaneza ei et. Al.	2014	problem of data security in cloud data storage.	RSA and AES encryption methods	Combination of asymmetric and symmetric keys with use of RSA and AES encryption algorithm to share the data among users in a secure cloud system.

III. SECURITY CHALLENGES

Internet is the key bone for Cloud computing environment and applications are deployed through public networks. With cloud applications, organizations can use services and data from any physical location. Outside access may be insecure and raise questions about privacy, confidentiality, integrity etc and demanded a trusted computing environment wherein data confidentiality, authentication with access control can be maintained.

The study of complete cloud environment raises certain issues which may be listed below;

- 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. Understanding of security threats in cloud computing environment for analyzing the requirement of security, certain security threats are observed those are described into Table II :

TABLE III Security Threats in Cloud Environment

Attack	Description
Tampering	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 kill or misuse the identity of node, server or client.
Viruses and Worms	Attacker may use certain bad source code to compromise

IV. PROBLEM STATEMENT

Cloud computing environment has wide application area and may deploy with various purpose. Although, security was primary concern since inception of internet due to its public connection, it becomes very critical due to involvement of internet with cloud computing. Cloud computing gives wide computing nature environment with distributed storage with parallel execution facility. It requires internet to enhance its scope from intranet to worldwide and uses internet services to access cloud application from outside the network. Any organization or computer node that process data through public network is subject for security breach and may be target for various security threats and attackers. It creates dilemma in user's mind about the trust and privacy of information. Any user who access or store their confidential information using cloud applications always required assurance about safety and security of content. The study of complete existing system explore that, existing solutions provides security but either one or two level. They do not gives complete security model or framework to integrate security with cloud applications. They address a very strong need of security model which should provide security not as the requirement but as essential component of application.

V. CONCLUSION

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. In a way to achieve its goal, the changed computing also demands some of modified operation of security control for more protection. In this paper a study of cloud security environment and requirement of cloud security has been explored and address with problem observations.

VI. REFERENCES

[1] Deyan Chen and Hong Zhao "Data Security and Privacy Protection Issues in Cloud Computing" 2012 IEEE International Conference on Computer Science and Electronics Engineering.

[2] Tumpe Moyo and Jagdev Bhogal "Investigating Security Issues in Cloud Computing" 2014 Eighth International Conference on Complex, Intelligent and Software Intensive Systems.

[3] Kai Hwang and Deyi Li "Trusted Cloud Computing with Secure Resources and Data Coloring" Published by the IEEE Computer Society 2010 IEEE INTERNET COMPUTING.

[4] 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.

[5] Cindhamani.J, Naguboynia Punya, Rasha Ealaruvi, L.D. Dhinesh babu "An enhanced data security and trust management enabled framework for cloud computing systems" IEEE 2014, Hefei, China.

[6] Pin Zhang, Jing Xu, Halilu Muazu, Wenmin Mao " Access Control Research on Data Security in Cloud Computing" Proceedings of ICCT 2015 IEEE.

[7] Nikhil Gajra ,Shamsuddin S. Khan and Pradnya Rane "Private Cloud Security:Secured user authentication by using Enhanced Hybrid Algorithm" 2014 International Conference IEEE.

[8] Mahnoush Babaeizadeh ,Majid Bakhtiari and Alwuhayd Muteb Mohammed "Authentication Methods in Cloud Computing: A Survey" Research Journal of Applied Sciences, Engineering and Technology 2015.

[9] B.Sumitra , C.R. Pethuru and M.Misbahuddin "A Survey of Cloud Authentication Attacks and Solution Approaches" International Journal of Innovative Research in Computer and Communication Engineering Vol. 2, Issue 10, October 2014.

[10] WhitePaper "MD5 Collisions" The effect on Computer Forensics 2015.