International Journal of New Technology and Research (IJNTR)
ISSN:2454-4116, Volume-3, Issue-4, April 2017 Pages 77-80

Security Issues in Cloud Computing

Rachit Singhal, Shivam Gupta, Rachna Jain

Abstract— Cloud computing is a paradigm that gives user an efficient and scalable business model to perform various technology functions like network, hardware, storage, bandwidth, software etc. Services are provided by some other company and these can be accessed over internet therefore it is just an alias of using computer hardware and software beyond firewall. Benefits include unlimited storage, universal access, collaboration, scalability and revolutionizing the way modern computing works. But with benefits comes the problems like organizations are transferring data and applications over cloud but security remains a very important concern. There are many threats related to cloud security like data loss, data breaches, malicious attacks, privacy etc. In this article we have studied the current problems in cloud security and proposed a security model using encryption techniques like SHA and RSA to tackle such situations.

Index Terms— Cloud Computing, Security, Encryption, SHA, RSA.

I. INTRODUCTION

Cloud computing is a model for sanctioning universal, available, on-demand network access to a proportional collection of configurable computing resources like, networks, servers, storage,, and services that can be immediately used and liberated using lower attempt or service provider interaction. In more simplified words cloud computing is referred as internet-based computing.

Cloud computing consists of three service models namely IaaS (Infrastructure as a Service), PaaS (Platform as a Service) and SaaS (Software as a Service). Saas represents the largest cloud market, instead of installation and maintainance of software users can connect to the project on the cloud based platform. It consists of a multitenant architecture wherein all users and applications share a single, common infrastucture environment that is preserved centrally. Examples of Saas includes Google Apps, Workday, Concur and Salesforce. Pass services are deployed in the cloud and can be accessed by the user from their internet browser. It makes the development, testing, and deployment of applications rapid, simple, scalable, reliable and cost-effective. Examples of Paas includes Salesforce, Heroku, AWS Elastic Beanstalk.. In Iaas a provides clients pay-as-you go access to storage, networking, servers and other computing resources. Examples vendor of Iaas includes Rackspace, Amazon Web Services, Cisco, Metapod, Microsoft Azure.

There are four deployment models in cloud, namely private cloud, public cloud, community cloud and hybrid cloud. In public cloud the infrastructure can be used by anyone which is provided by a third party cloud service provider. In private cloud infrastructure can be used only by a single organization. Community cloud is an extension of private cloud where the cloud is owned, used and managed by more than one organization and hybrid cloud is a composition of two or more than two distinct cloud infrastructures which can be public, private and community.

The growing popularity of cloud computing can be accredited to the following advantages offered [3] - 1. On Demand Self-Service: The service provided is automatic and does not require human interaction. 2. Broad Network Access: Services are accessed over the network and hence can be used for any device and any location. 3. Resource Pooling: Using multi-tenant model, CSP's resources are pooled to serve multiple customers. 4. Rapid Elasticity: The resources can be rapidly scaled (inward or outward) depending on the demand. 5. Measured Service: The usage of various resources is monitored, checked and reported by the CSP.

II. THREATS TO CLOUD SECURITY

A. *Data Breaches*

If a cloud service is not properly designed and architecture, then the system will become vulnerable towards security threats which can cause the stealing of client's data like passwords, pins etc.

B. *Data Loss*

Data breach is the result of an attacker's malicious and intrusive action. Data loss occurs when user looses the encryption key or a disk drive dies.

C. *Account or Service Traffic Hijacking*

Buffer flow attacks, loss of passwords and other very important credentials can lead to a loss of control over account which may lead to account hijacking. Wrong parties can access the user data in an unwanted way. Recently amazon.com experienced a cross site scripting attack.

D. *Insecure APIs*

API defines how a party can connect to service without going into background details of how it is made. Generally APIs are not secured and developers use them in their program which makes system vulnerable to security issues. OAuth controls this third party access but it can be tricked as well.

E. *Denial of Service*

Attackers use this approach to breach security parameters where the users are caught in a rush-hour traffic gridlock. They just have to sit and wait and in the meantime cloud service provider charges the user for all the resources that are

Rachit Singhal, Computer Science Department, Bharati Vidyapeeth's College of Engineering, New Delhi, India.
Shivam Gupta, Computer Science Department, Bharati Vidyapeeth's College of Engineering, New Delhi, India.
Rachna Jain, Computer Science Department, Bharati Vidyapeeth's College of Engineering, New Delhi, India.

being used during attack.

F. Malicious Insiders

If all the keys are kept with the cloud service provider then the security of system is at a great risk. System will be prone to malicious insider attack if the keys are only available at data usage time and not with users.

G. Abuse of Cloud Services

It might be impossible for a hacker to decrypt an encryption key using his limited hardware, but it will be easier using an array of cloud servers and distribute many attacks like DDoS, distribute pirated software etc.

H. Shared technologies and Dangers

Cloud service providers generally share various resources like architecture, infrastructure, platforms etc. If any one layer is affected then the whole system will be affected. Whole system will be exposed to risk if anything is compromised.

I. Inadequate Diligence

Organizations that use the cloud services without fully understanding it may encounter problems like commercial, financial, technical, legal etc. They must perform due diligence to avoid the risks that they may face while using the cloud services.

III. RELATED WORK

Various studies and researches are done in the field of cloud security. Some of these have been discussed in the following section. Joshi M et al[6] proposed the architecture for a virtual private storage service which is based on cryptographic techniques on both consumer and enterprise level.. Ahmadi M.et al[7] proposed a user authentication model where two encryption procedures AES and RSA have been established in an Agent(an independent middleware between the end-user and cloud servers) to perform various functions like user authentication, access control, etc. in cloud servers. AES is used as a symmetric cryptography algorithm in cloud servers and RSA is used as an asymmetric cryptography algorithm in Agent servers. The model can protect from attacks like Man in the Middle attack and Discrete Logarithm attack.

Naik NV et al[8] proposed the introduction of third party auditor in between the client and the cloud server to help the client to frequently check the integrity of data stored in cloud.

Veeraragavan N et al[9] put forward a framework VEARAaaS consisting of three components, Authenticator, Encryptor and Key generator. Authenticator is used for verifying the user, the encryptor is used to encrypt the registration data of the user prior to storing the data and Key Generator is used to generate a key for encryption and authentication service.

Kumar S et al[10] put forward a two tier authentication scheme using the user's personal device having a unique id. The first tier includes username and password authentication. In the second tier of authentication, One-Time Password (OTP) is sent from the server to the registered device.

Sulochana V et al[11] proposed a puzzle based authentication scheme in which the user registers and solves the puzzle, puzzle solving time and sequence of image block is stored and validated by local server and the user gets successfully authenticated.

Yan L, Rong C, Zhao G.[12] adopted a federated identity management along with hierarchical identity-based cryptography (HIBC) for both mutual authentication and key distribution. Federated identity management is a method for different establishments to share user and service identity.

Goswani B et al[13] proposed a three-stage secured algorithm. The first stage includes shuffling of data using the linear congruential method followed by arranging the data in a matrix form. In the second stage, the matrix is transversed in different forms like helical, spiral, etc. Finally, the third stage deals with generating a system of non-homogeneous linear equations from which private keys are generated.

Squicciarini A, Sundareswaran S, Lin D.[14] designed a three-tier data protection architecture which has been used to accommodate different levels of privacy concerns by users. They developed a novel portable data binding technique to make sure that there is strong enforcement of users' privacy requirements. It introduces very less overhead.

Nagamani V et al[15] contemplated a design in which data is stored on the cloud in an encrypted format and a set of secret keys, implementing variable size cryptosystem, are used as a single aggregate key to decrypt the data. A key hierarchical structure is used for generation of key. The data is searched for a set of attributes, these attributes are arranged in a hierarchical structure which is further used to generate the aggregate key.

Tirodkar S et al[16] proposed a two phase, 3 dimensional architecture for ensuring security of data on cloud. The first phase deals with encryption and classification of data into three protection rings, with the innermost protection ring, protection ring 1, containing the most sensitive data. This classification is based on the following factors, Confidentiality, Integrity and Availability .The second phase deals with data retrieval. Depending on the layer accessed, a different mechanism is used to verify the user's identity. The outermost ring, protection ring 3 is authenticated using username and password, protection ring 2 uses graphical password authentication and protection ring 1 is authenticated using an OTP sent to the user's device. Finally, the retrieved data is decrypted using the decryption key. The architecture provides security from DDOS attacks and data leakage. However, the introduction of OTP and use of hardware devices for authentication introduces complications.

Ullah S et al[17] set forth a two module architecture consisting of client and server module. The main purpose of the client model, consisting of Multi-Purpose Access Module, Split/Merge Module and Encryption Module is to verify the user and encrypt or decrypt data for storing and retrieving the data respectively.

Shyamala MG et al[18] put forward a two module, multi-level authentication architecture to ensure confidentiality and integrity of data. The proposed architecture is very simple and highly secure.

Singh M et al[19] proposed a two tier authentication process where the first tier uses traditional encryption

decryption mechanism and in the second tier the user is required to perform a certain sequence of predetermined activities on the fake screen.

Agme VS et al[20] proposed a secure cloud system where the permission for a given file or document is dependent not only on the identity of the person but the file as well. The data is encrypted and stored on the cloud by the owner. When a user requests access to a file, the owner gets notified.

Rewagad P et al[21] provided a three way mechanism ensuring authentication, data security as well as verification. The mechanism uses digital signature and Diffie Hellman algorithm for key generation along with AES encryption algorithm for encryption and decryption of data.

Casola V et al[23] put forward a framework that enables the adoption of a pre-service SLA model. The framework consists of building a list of security mechanisms which implement a set of security policies and offering them as-a-service.

Warhade RG et al[24] proposed a Identity based multi-cloud storage scheme(IBMCSS) where the data is split , encrypted and stored on multiple clouds . In this scheme, the data is first split into chunks, then each chunk is encrypted using AES algorithm and finally the data is stored on multiple clouds.

IV. PROPOSED MODEL

RSA is a cryptographic system used for encryption so as to send sensitive data over network. It is asymmetric cryptography using two keys i.e. private and public keys. It provides a method of assuring the confidentiality, integrity, authenticity and non- reputability of electronic communications and data storage. Both the public and the private keys can encrypt a message; the opposite key from the one used to encrypt a message is used to decrypt it.

Our model focuses on providing greater security to the client by granting three tier security. First tier deals with the username and password authentication, wherein details entered by user are matched with the values stored in database. In the Second tier authentication, OTP is sent from server to the registered email-id. Third level authentication includes email verification. This system uses three softwares to provide encryption decryption functionalities.

Firstly the OTP is passed into the first software which will generate an encrypted key using RSA encryption. This encrypted key is combined with the encrypted data encrypted using RSA algorithm and is sent to second software as an input which generates the decrypted data and stores on the cloud. Now the user data is safely stored on the cloud for accessing the data, software is used which will decrypt the user data stored on cloud using RSA decryption algorithm.

Using this model, two tier authentication can be made possible which is valid for single session. Encrypted data is stored on the cloud which enhances the security level of the system. Strong encryption and decryption techniques are used to generate private and public keys. It ensures confidentiality of data, availability of data, protection from various attacks like man in middle attack, tampering attack, online attack etc.

First Tier- Username and Password Authentication

Second Tier- OTP Authentication

Third Tier- Email Verification

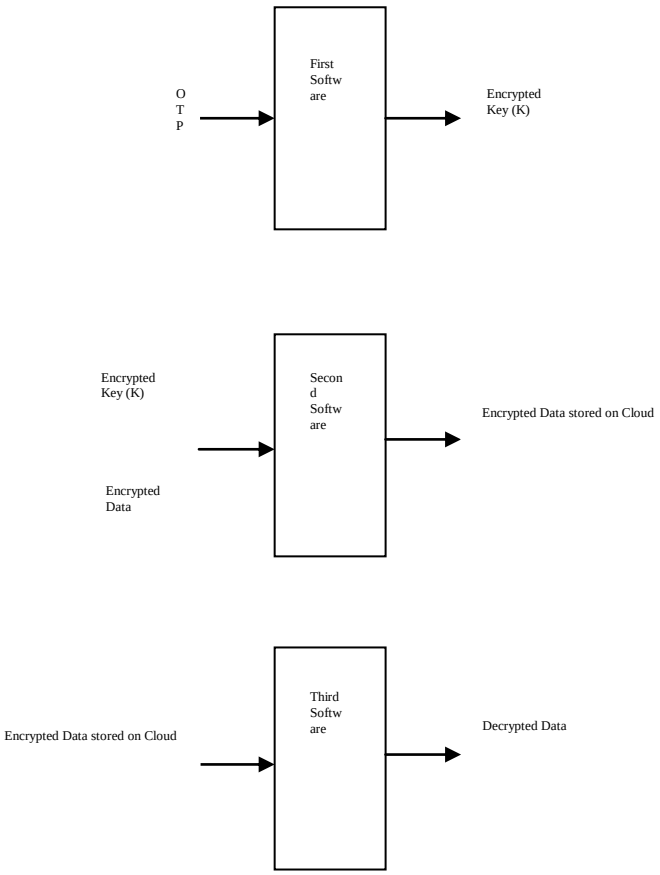

Fig:1

V. CONCLUSION AND SCOPE

This paper has reviewed overall concept of cloud computing and its associated risks. According to our analysis, multitier authentication system offers more security over single tier systems. Our Security Model promises a great level of security which can prove to be a big milestone in the field of cloud security. Future work can be done to develop more complex security systems which will safeguard the client as well as server from more threats.

REFERENCES

[1] Armbrust M, Fox A, Griffith R, Joseph AD, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I, Zaharia M. A view of cloud computing. Communications of the ACM. 2010 Apr 1;53(4):50-8.
[2] Mell P, Grance T. The NIST definition of cloud computing.
[3] Subashini S, Kavitha V. A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications. 2011 Jan 31;34(1):1-1.
[4] Kilari N, Sridaran R. An Overview of DDoS Attacks in Cloud Environment. International Journal of Advanced Networking & Applications. 2015 May 2.
[5] Singh A, Shrivastava M. Overview of attacks on cloud computing. International Journal of Engineering and Innovative Technology (IJEIT). 2012 Apr;1(4).
[6] Joshi M, Moudgil YS. Secure cloud storage. International Journal of Computer Science & Communication Networks. 2011 Oct;1(2):171-5.
[7] Ahmadi M, Vali M, Moghaddam F, Hakemi A, Madadipouya K. A Reliable User Authentication and Data Protection Model in Cloud Computing Environments. arXiv preprint arXiv:1508.01703. 2015 Aug 7.

[8] Naik NV, Priyanka D. Affording Greater Privacy in Cloud Storage Auditing with Random Masking Technique. International Journal of Research. 2016 Jul 25;3(11):946-50.
[9] Veeraragavan N, Arockiam L. A Novel Framework for Authentication as a Service (AaaS) in Public Cloud Environment.
[10] Kumar S, Ganpati A. Multi-authentication for cloud security: A framework. International Journal of Computer Science & Engineering Technology. 2014 Apr;5(4):295-303.
[11] Sulochana V, Parimelazhagan R. A puzzle based authentication scheme for cloud computing. International Journal of Computer Trends and. 2013 Dec:210-3.
[12] Yan L, Rong C, Zhao G. Strengthen cloud computing security with federal identity management using hierarchical identity-based cryptography. InIEEE International Conference on Cloud Computing 2009 Dec 1 (pp. 167-177). Springer Berlin Heidelberg.
[13] Goswani B, Singh DS. Enhancing security in cloud computing using public key cryptography with matrices. International Journal of Engineering Research and Applications. 2012 Jul;2(4):339-44.
[14] Squicciarini A, Sundareswaran S, Lin D. Preventing information leakage from indexing in the cloud. In2010 IEEE 3rd International Conference on Cloud Computing 2010 Jul 5 (pp. 188-195). IEEE.
[15] Nagamani V, Rao VV, Rao MV. Secure Scalable Data Sharing in Cloud Storage using Randomized Key Aggregate Crypto System. Global Journal For Research Analysis. 2016 Jul 9;4(7).
[16] Tirodkar S, Baldawala Y, Ulane S, Jori A. Improved 3-Dimensional Security in Cloud Computing. arXiv preprint arXiv:1404.1836. 2014 Apr 7.
[17] Ullah S, Xuefeng Z. TCLOUD: A Trusted Storage Architecture for Cloud Computing. International Journal of Advanced Science and Technology. 2014 Feb;63:65-72.
[18] Shyamala MG, Narmada B, Nivetha SM. A Trusted Storage and Data Retrieval in Cloud Computing. History. 2015;34(154):43-7.
[19] Singh M, Singh S. Design and implementation of multi-tier authentication scheme in cloud. International Journal of Computer Science Issues. 2012 Sep;9(5):181-7.
[20] Agme VS, Lomte AC. Cloud Data Storage Security Enhancement Using Identity Based Encryption. Identity. 2014 Apr;3(4).
[21] Rewagad P, Pawar Y. Use of digital signature with Diffie Hellman key exchange and AES encryption algorithm to enhance data security in cloud computing. InCommunication Systems and Network Technologies (CSNT), 2013 International Conference on 2013 Apr 6 (pp. 437-439). IEEE.
[22] Sarkar MK, Chatterjee T. Enhancing Data Storage Security in Cloud Computing Through Steganography. International Journal on Network Security. 2014 Jan 1;5(1):13.
[23] Casola V, De Benedictis A, Modic J, Rak M, Villano U. Per-service Security SLA: a New Model for Security Management in Clouds. InEnabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), 2016 IEEE 25th International Conference on 2016 Jun (pp. 83-88). IEEE.
[24] Warhade RG, Vankudothu B. Enhancing Cloud Security Using Multicloud Architecture and Device Based Identity. In2015 7th International Conference on Emerging Trends in Engineering & Technology (ICETET) 2015 Nov 18 (pp. 34-39). IEEE.
[25] Jung T, Li XY, Wan Z, Wan M. Control cloud data access privilege and anonymity with fully anonymous attribute-based encryption. IEEE Transactions on Information Forensics and Security. 2015 Jan;10(1):190-9.
[26] Dong X, Yu J, Luo Y, Chen Y, Xue G, Li M. Achieving an effective, scalable and privacy-preserving data sharing service in cloud computing. computers & security. 2014 May 31;42:151-64.