ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

The Integrated and Improved Framework for Cloud Data Security: A Survey

Rajeev Ranjan[1], Ashok Verma[2]

M.Tech Student, Dept. of CSE, GGITS, JBP, India.[1]

Assistant Professor, Dept. of CSE, GGITS, JBP, India.[2]

ABSTRACT: Cloud owners provide various promising services to users and this makes the cloud to be very popular among users. Despite of the several benefits of migrating enterprise critical assets to the Cloud, there are challenges specifically related to security and privacy. Cloud computing is a location independent computing wherein files are outsourced as a service. Users outsource their data to the third party cloud server to reduce various costs such as storage, management etc. The outsourced data may have sensitive and valuable information that needs to be secured. In order to assure confidentiality, users encrypt their data before outsourcing it to the cloud server. With integrating into cloud computing, security issues such as data confidentiality and user authority may arise, and it is concerned as the main constraints to the developments of cloud computing. Proposed framework can protect data while transferring, sharing and storing in data centres using advanced encryption of data. It also focuses on multi-factor authentication that maintains legal authority to the data.

KEYWORDS: Secure Storage, OTP, MFA, Data Integrity and Authentication

I. INTRODUCTION

Cloud computing is a model for providing convenient on demand network access to a shared pool of computing resources. It provides resources dynamically whenever demanded by the user. The resource is utilized by the user without having enough knowledge about the technical details involved in the resource provider. Cloud Computing is a model of computing, not a technology. In this scheme "customers" plug into it to access various resources which are priced and provided "on-demand ".Cloud computing offers on-demand services in the form of infrastructure, platform and software to users in rent based model. Its great scalability, flexibility and on-demand cost motivates users to outsource their files to the cloud as the need to storage and retrieval of information became increasingly important [1].
Along with it Security is a great issue for cloud computing. The three main security goals confidentiality, integrity, and availability should be incorporated in the cloud system [2]. For a secure cloud computing protection is needed for user identity, their data, and server data privacy. Data can be stolen during transmission as well as at the time of storing on the server. There are lots of security risks associated with cloud computing. This paper presents a survey on all possible security issues of cloud environment and feasible remediation.

CLOUD SERVICE MODELS

i) Iaas: IaaS offers virtualized resources on demand. These virtualized resources include storage, communication and computation. It is the bottom layer of the cloud stack.E.g of IaaS includes Amazon EC2, Flexiscale, Joyent, GoGrid, and Rackspace.

ii) Platform as a Service: It offers a higher level of abstraction which makes cloud easily programmable. This is known as Platform as a Service (PaaS). A cloud platform offers an environment on which developers create and deploy applications and do not necessarily need to know how many processors or how much memory that applications will be used. E.g of IaaS includes Aneka, Google App Engine and Microsoft Azure.

iii) Software as a Service: Applications reside on the top of the cloud stack. End users access the services provided by SaaS through Web portals .E.g of SaaS includes Salesforce.com, Google app, Facebook, youtube.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

CLOUD DEPLOYMENT MODELS

i) **Private Cloud**: The cloud infrastructure is an internal data center of an organization which is not meant for the general public. It is used by a single organization consisting of multiple consumers (e.g., business units).
Private clouds may be owned and managed by an organization or a third party. It may exist on or off premises.
ii) **Public cloud**. The cloud infrastructure is made available to the general public on a pay-as-you-go basis. It may be owned, managed and operated by a government organization business organizations and academic organizations. It exists on the premises of the cloud provider.
iii) **Community cloud**. The cloud infrastructure is shared by several organizations and supports a specific community that share common goals. It may be owned, managed, and operated by any organization in the community or a third party. It may exist on or off premises.
iv) **Hybrid cloud**. The cloud infrastructure is a combination of two or more clouds (private, community, or public).

SECURITY CHALLENGES AND THREATS IN CLOUD COMPUTING

There are certain principles which we need to abide by so as to have a secure cloud communication. These principles are referred as Information Security Principles. CIA Triad is a well known security model which deals with important aspects of IT security. It is used to identify security problems and provide its necessary solutions [3, 4]. In the CIA Triad, C stands for Confidentiality, I for Integrity and A stands for Availability. These security principles are also discussed in [5].
i) Confidentiality - Confidentiality refers to protecting the information from unauthorized users. Its aim is to ensure that information is hidden from unauthorized users to access it. With the increase in number of applications and equipments in cloud, threats also increases which lead to an increased number of access points.
ii) Integrity - Integrity refers to the consistency and accuracy of data. The data should not be modified by any unauthorized user or in an unauthorized manner. It says that data should not be altered in transit.
iii) Availability - The principle of availability says that the information must be available whenever it is needed. It refers to the property that the system must be usable and accessible when requested by the authorized users.

II. RELATED WORK

Nowadays, cyber warfare is arguably the most complex challenge in a distributed and multi- tenant environment. It is a complex job within the client-server architecture. When the data transfer to the cloud services, the requirements of security should be the most important. The European Network Information Security Agency (ENISA) enumerated the risks, recommendations and benefits for cloud computing [6]. It also lists the infection on confidential document, loss of governance, malicious insider, and insecure incomplete data. The Elastica 2015 shadow data report [7] it focuses on unauthorized apps discovered in an organization.
In this section, we briefly introduce about the major security concerns of cloud computing.
Storage security: In cloud storage system, end user stores the data in the cloud and no longer owns the data and where it's stored. This always has been an important aspect of quality of service. It ensures the correctness of user's data in the cloud and by utilizing homomorphism token with distributed verification of erasure-coded data [8]. Storage security concerns about data sanitization, cryptography, data-Remanence, data leakage, snooping of data availability and malware.
Network security: In cloud computing, communication is via the internet and it is the backbone of the cloud environment. Network security concerns about both internal and external attacks. These attacks in the network can either occur in the virtual or physical network. Yuhong Liu W., et al. [9] focuses on the virtual network in a Xen platform by discussing and analyzing its security problems.
Security issues in the cloud environment are caused by its essential characteristics such as resource pooling, virtualized nature, elasticity, and some measured services. There was an increase of 70% Advance Persistence Threat (APT) attacks [10], 68% suspicious activities, and 56% brute force attacks on a cloud environment in 2015. APT attack is network attack in which an unauthorized identity gain access to a network and remain undetected for a long period.
Yuhong L., et al. [9] surveyed critical privacy and security challenges in cloud computing, categorized diverse existing solutions, compared their strengths and limitations, and envisioned future research directions.
Zhaolong G., et al. [7] discussed recent developments in cloud computing, various security issues and challenges in cloud computing environment, various existing approach and solutions provided for dealing with these security threats.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

Zhifeng and Yang [11] provided a systematic review of security issues in clouds based on an attribute-driven methodology. The attributes used were confidentiality, integrity, availability, accountability, and privacy-preservability. For each attribute, a few threats were reviewed along with the corresponding defence solutions.
Ning C., et al. [12] proposed a Multi-key word Ranked search Scheme over Encrypted (MRSE) cloud data to provide better privacy preserving. This paper through analysis investigating privacy and efficiency guarantees the proposed scheme.
Qin L., et al [13] proposed the time based proxy-re encryption for data sharing in a cloud environment. The aim of this scheme is to encrypt the data before outsourced it. Key generation, Proxy Re-Encryption (PRE), attribute-based encryption, the bilinear map is used to demonstrate to provide fine-grained access control on encrypted data, scalable user revocation, authentication and confidentiality of cloud data. To enhance the security mechanism of identity and access management in the cloud proposed in reference [14]. The author combines the Elliptical Curve Cryptography (ECC) technology for low key size but high-security level with robust nature and Identity-Based Cryptography (IBC) to reduce key management complexity using trusted cloud. The enhance IAM mechanism provide a high level of authentication, robustness less cost and efficient revocation management. The ECC implemented with a 160-bit key size that offers same security level against 1024-bit key size of RSA cryptosystem that makes IAM more efficient. L.in, et al. [15] presented a technique of identity-based encryption that simplifies public key management and certificate in Public Key Infrastructure (PKI), which is alternative to public key encryption. The basic theory in this paper public key generator, key service procedure in which key issue and update processing technique were utilized and two
cryptographic background techniques Bilinear map and decision bilinear Diffie-Hellman problem is proposed in IBE. The paper also provides the computational-experimental result to determine the cost and time efficiency of proposed model. Sandeep K.S., et al. [16] gave the idea of combined approach to ensure the data security in the cloud that focuses on the basic security attribute such as confidentiality, integrity, availability, and authentication and provide user identity and password. The concept followed to secure the data 128-bit and 256-bit SSL encryption and MAC for integrity check and double authentication of user one by the owner of data and another is by cloud.
For the better enhancement for cloud data security using digital signature concept with Diffie-Hellman key exchange and AES encryption is proposed in [17]. The proposed architecture utilizes ECDH that generates the key for key exchange and then digital signature is used to authenticate the data after that AES algorithm is used for encryption/decryption by session key to avoiding MIM attack and maintain the integrity of data [18].

III. PROPOSED MODEL

The proposed model consists of following phases:

1. Registration Phase: User will register by entering some required credentials.
2. Entered Information will be stored in cloud database using ECC as a encryption method.
3. OTP will be generated.
4. Re-Authentication using OTP
5. Validate using Digital Certificate

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

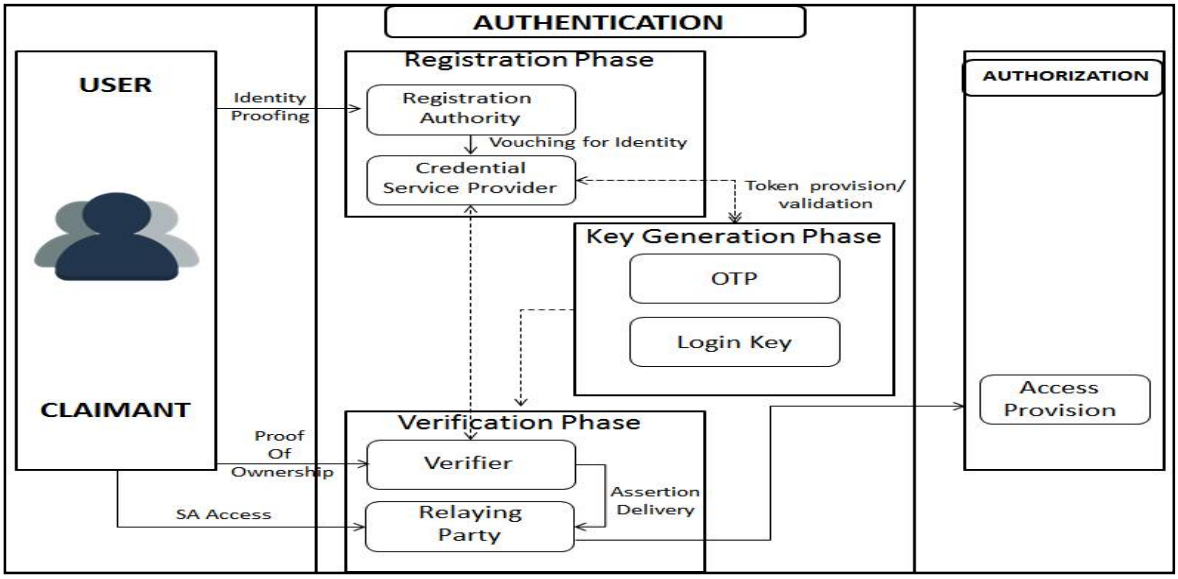

Fig. 1: Block Architecture of proposed system

IV. CONCLUSION

The hype of cloud paradigm is changing the IT industry; it brings many benefits to companies, organizations and even countries. Despite bringing several advantages, the cloud still is vulnerable to many security challenges.
This research attempted to show various security challenges, vulnerabilities, attacks and threats that hamper the adoption of cloud computing. Our paper provided a state-of–art survey on cloud security issues and challenges that arise from unique characteristics of the cloud like authentication, integrity of data and its availability. We have proposed the Multi-tier security architecture for better security enhancement of cloud security. we explore the feasibility of introducing MFA to ensure authentication for cloud access control as Multiple factors raise the threshold for successful attacks.

REFERENCES

[1]. S. Kamara and K. Lauter, "Cryptogra(Jhic Cloud Storage," Proc. 14th Int'l Conf. Financial Cryptograpy and Data Security, Jan. 2010.
[2]. Asish Aich, Alo Sen, Satya Ranjan Dash A Survey on Cloud Environment Security Risk and Remedy International Conference on Computational Intelligence & Networks.vol 2,Issue 4, Jun 2015.
[3]. http://www.techrepublic.com/blog/it -security/the-ciatriadl.
[4]. http://www.slideshare.net/bharathraob/the-cia-triad -28739772.
[5]. Mircea Georgescu, Natalia Suicirnezov, "Issues Regarding Security Principles In Cloud Computing",The USV Annals of Economics and Public Administration Volume 12, Issue 2(16), 2012.
[6]. Sudhir N. Dhage, B. B. Meshram, "Intrusion detection system in cloud computing environment," International Journal of Cloud Computing, Vol. 1, Issue 2-3, pp. 261-282, 2012.
[7]. Zhaolong Gou, Shingo Yamaguchi, B. B. Gupta. "Analysis of Various Security Issues and Challenges in Cloud Computing Environment: A Survey", In Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security, IGI Global, pp. Vol 4, May 2016.
[8]. Nguyen, Thanh Cuong, Wenfeng Shen, Zhaokai Luo, Zhou Lei, and Weimin Xu. "Novel Data Integrity Verification Schemes in Cloud Storage." In Computer and Information Science, Springer International Publishing, Vol 5,April-2015.
[9]. Yuhong Liu, Yan Lindsay Sun, Jungwoo Ryoo, Syed Rizvi, and Athanasios V. Vasilakos. "A Survey of Security and Privacy Challenges in Cloud Computing: Solutions and Future Directions." Journal of Computing Science and Engineering, Vol. 9, Issue. 3,Jul- 2015.
[10]. Martin Ussath, David Jaeger, Feng Cheng, Christoph Meinel. "Advanced persistent threats: Behind the scenes." IEEE, Annual Conference on Information Science and Systems (CISS), Vol 6,Jan 2016.
[11]. Zhifeng, Xiao, and Yang Xiao. "Security and privacy in cloud computing",Communications Surveys & Tutorials, IEEE, Vol. 15, Issue 2, Dec 2013.
[12]. Ning Cao, Cong Wang, Ming Li, Kui Ren, Wenjing Lou,"Privacy-preserving multi-keyword ranked search over encrypted cloud data," IEEE Transactions on Parallel and Distributed Systems,Vol. 25, Issue 1,Mar 2014.
[13]. Qin Liu, Guojun Wang, Jie Wu, "Time-based proxy re-encryption scheme for secure data sharing in a cloud environment," Information Sciences,ELSEVIER, Vol. 258, Aug 2014.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

[14]. Salim Ali Abbas,“ Enhancing the Security of Identity and Access Management in Cloud Computing using Elliptic Curve Cryptography”,International Journal of Emerging Research in Management &Technology, Vol.4, Issue. 7, 2015.
[15]. Li, Jin, Jingwei Li, Xiaofeng Chen, Chunfu Jia, and Wenjing Lou. "Identity-based encryption with outsourced revocation in cloud computing."Computers, IEEE Transactions on, Vol. 64, Issue. 2, 2015.
[16]. Sandeep K Sood,“A combined approach to ensure data security in cloud computing,” Journal of Network and Computer Applications, vol. 35,Issue 6,Nov. 2012.
[17]. Rewagad, Prashant, and Yogita Pawar. "Use of digital signature with diffie hellman key exchange and AES encryption algorithm to enhance data security in cloud computing." International Conference on Communication Systems and Network Technologies (CSNT), IEEE, 2013.
[18]. Nidal Hassan Hussein, Ahmed Khalid, Khalid Khanfar, "A Survey of Cryptography Cloud Storage Techniques", 2016.

BIOGRAPHY

Rajeev Ranjan is a Research Scholar in the Computer Science Department, Gyan Ganga Institute of Science & Technology, Jabalpur, and M.P.