ISSN 2320-9984

Volume 3 Issue 1 | March 2015

ISSN: 2320-9984 (Online)

International Journal of Modern Engineering & Management Research

Website: www.ijmemr.org

An Extensive Survey Expounding Security Issues & Requirement in Secure Cloud Computing Environment

Manish Mishra
Research Scholar
Department of Computer Science & Engineering
Jai Narain College of Technology
Bhopal (M.P.), [INDIA]
Email:redefine_manish@yahoo.com

Dr. Mukta Bhatele
Head of Department
Department of Computer Science & Engineering
Jai Narain College of Technology
Bhopal (M.P.), [INDIA]
Email: mukta_bhatele@rediffmail.com

Abstract—*The use of cloud computing has increased rapidly in many organizations. Cloud computing provides many benefits in terms of low cost and accessibility of data. Ensuring the security of cloud computing is a major factor in the cloud computing environment, as users often store sensitive information with cloud storage providers but these providers may be untrusted. Since cloud computing share disseminated resources via the network in the open environment, hence it makes security problems vital for us to develop the cloud computing applications. Cloud computing security has become the leading cause of hampering its development. Cloud computing security has become a hot topic in industry and academic research. This paper has made an extensive survey over existing approaches which secures the environment and also propounded a framework to be implemented to secure data outsourcing by deploying identity based encryption using Elliptic curve cryptography, and the same is being evaluated on the basis of different parameters.*

Keywords:—*Cloud computing, Security, Encryption, Decryption, Elliptic Curve Cryptography (ECC).*

1. INTRODUCTION

Cryptography has evolved from the earliest forms of secret writing to current era of computationally secure protocols, addressing range of security issues. In modern age, cryptography is not only about encryption, but it has larger objective of ensuring data protection from adversary’s activities. Scope of modern cryptography also includes techniques and protocols to achieve authentication, non-repudiation, and integrity objectives. Complexity of cryptology methods and its applications have continuously increased and evolution of computers has given a completely new dimension to this. Now cryptography problems/algorithms are measured in terms of computational hardness. In this journey, cryptography has always received a threat of getting obsolete because of rapidly increasing computational capabilities. However, cryptography techniques still have great relevance and importance for modernICT (Information and Communication Technology), and ICT enabled industry to keep them protected from dynamically changing threat scenarios.

It is a tool for providing simple, needed network access to shared resources of configurable computing environment (network, storage etc) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Today most of the companies have to process huge amounts of data in a cost-reducing manner. Classic users are operators of

Internet search engines such as Google, Yahoo, or Microsoft. The vast amount of data they have to deal with every day has made database solutions more expensive.

Cryptography is the science of encrypting information. It provides the services of confidentiality, integrity and non-repudiation to support information protection. In general, these services are realized by two cryptographic primitives. The encryption primitives can be used to provide confidentiality and the authentication primitive can be used to provide data integrity and non-repudiation. Few most popular encryption schemes are AES, DES, SHA, IDEA, RC5, RSA, ECC etc.

2. CLOUD COMPUTING

A cloud typically contains a virtualized significant pool of computing resources, which could be reallocated to different purposes within short time frames. The entire process of requesting and receiving resources is typically automated and is completed in minutes. The cloud in cloud computing is the set of hardware, software, networks, storage, services and interfaces that combines to deliver aspects of computing as a service. Share resources, software and information are provided to computers and other devices on demand.

2.1 Related Concepts

2.1.1 Deployment Cloud Models

Public Cloud: The cloud infrastructure is made available to the general public people or a large industry group and provided by single service provider selling cloud services.

Private Cloud: The cloud infrastructure is operated solely for an organization. The main advantage of this model is the security, compliance and QoS.

Community Cloud: The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns like security requirements, policy, and compliance considerations.

Hybrid Cloud: the cloud infrastructure is a combination of two or more clouds. It enables data application portability through load balancing between clouds.

2.1.2. Cloud Characteristics

- On demand service.
- Ubiquitous network access.
- Easy use.
- Business model.
- Location independent resource pooling.

2.1.3. Cloud Solutions

- Infrastructure as a service (IaaS)
- Software as a service (SaaS)
- Platform as a service(PaaS)

3. CLOUD SECURITY CHALLENGES

The cloud services present many challenges to an organization. When an organization mitigates to consuming cloud services, and especially public cloud services, much of the computing system infrastructure will now under the control of cloud service provider. Many of these challenges should be addressed through management initiatives. These management initiatives will requires clearly delineating the ownership and responsibility roles of both the cloud provider and the organization functioning in the role of customer. Security managers must be able to determine what detective and preventative controls exist to clearly define security posture of the organization. Here are security risks list.

Regulatory Compliance: Cloud computing providers who refuse to external audits and security certifications.

Privileged User Access: Sensitive data processed outside the organization brings with it an inherent level of risk.

Data Location: When you use cloud, you probably won't know exactly where your data hosted.

Data Segregation: data in the cloud is shared environment alongside data from other customers.

Recovery: even if you don't know where your data is, a cloud provider should tell you what will happen to your data and service in case of a disaster.

Investigative Support: investigating inappropriate or illegal activity may be impossible in cloud computing.

Long Term Viability: you must be sure your data will remain available even after such an event.

4. ELLIPTIC CURVE CRYPTOGRPAHY

Elliptic Curve (EC) systems as applied to cryptography were first proposed in 1985 independently by Neal Koblitz and Victor Miller. An elliptic curve over a field K is a nonsingular cubic curve in two variables, f(x,y) =0 with a rational point (which may be a point at infinity). The field K is usually taken to be the complex numbers, reals, rationals, and algebraic extensions of rationals, p-adic numbers, or a finite field. Elliptic curves groups for cryptography are examined with the underlying fields of Fp

$$y^2 = x^3 + ax + b$$

(where p>3 is a prime) and F2m (a binary representation with 2m elements). An elliptic curve is a plane curve defined by an equation of the form Consider elliptic curve

$$E: y^2 = x^3 - x + 1$$

If P1 and P2 are on E, we can define addition P3 = P1 + P2

As shown in picture below, let P1=(x_1, y_1), P2=(x_2, y_2) and P3=(x_3,y_3) and P1≠P2.

$$m = \frac{y_2 - y_1}{x_2 - x_1}$$

To find the intersection with E, we get

$$(m(x - x_1) + y_1)^2 = x^3 + Ax + B$$

or

$$0 = x^3 - m^2x^2 + \cdots$$

So,

$$x_3 = m^2 - x_1 - x_2$$

$$=> y_3 = m(x_1 - x_2) - y_1$$

Multiplication is defined as repeated addition. Elliptic curve cryptography [ECC] is a public-key cryptosystem. Every user has a public and a private key. Public key is used for encryption/signature verification. Private Key is used for decryption/signature generation.

4. EXISTING WORK

AlZain et al made a survey and suggested research related to single and multi-cloud security and addresses possible solutions. He proposed and supported the migration to multi-clouds due to its ability to decrease security risks that affect the cloud computing user[1].

Sharma B. introduces the existing issues in cloud computing along with network security and proposed a security framework to achieve secure cloud platform using Elliptic Curve Cryptography[2].

Venkataramana, K.&Padmavathamma M. proposed an another security architecture in which they have used threshold data sharing technique to be used in federation of clouds which allows data privacy and security in transit between them[3].

Buyya et al. in suggests a cloud federation oriented, just-in-time, opportunistic and scalable application services provisioning environment called InterCloud. As a result Cloud application service (SaaS) providers will have difficulty in meeting QoS expectations for all their consumers. Hence, they would like to make use of services of multiple Cloud infrastructure service providers who can provide better support for their specific consumer needs. This kind of requirements often arises in enterprises with global operations and applications such as Internet service, media hosting, and Web 2.0 applications. This necessitates building mechanisms for federation of Cloud infrastructure service providers for seamless provisioning of services across different Cloud providers[4].

Even within the cloud provider's internal network, encryption and secure communication are essential, as the information passes between countless, disparate components through network domains with unknown security, and these network domains are shared with other organizations of unknown reputability[6].The confidentiality of sensitive data must be protected from mixing with network traffic with other cloud hosts. If the data is shared between multiple users or clouds, the CSP must ensure data integrity and consistency. The CSP must also protect all of its cloud service consumers from malicious activities or data modification[7].

Subashini and Kavitha, has discussed various security issues at various service models like Data, Network security, Data locality & integrity, Data segregation, Data access, Authentication and authorization. In the case of federated clouds this becomes more serious issue that is to be addressed. For computation exchange of data between clouds in federation is necessary so both privacy and integrity of data should be considered[5].

Li et. Al in their paper proposed an approach to secure Personal Health records over Cloud environment by using attribute based encryption and focus on the multiple data owner scenario, and divide the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users. A high degree of patient privacy is guaranteed simultaneously by exploiting multi-authority ABE. This scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/ attribute revocation and break-glass access under emergency scenarios. Extensive analytical and experimental results are presented which show the security, scalability, and efficiency of the proposed scheme[8].

Sudha, M., & Monica, M. investigated the existing security schemes to ensure data confidentiality, integrity and authentication. They have employed RSA and AES and SHA algorithms to expound a hybrid security structure for cloud computing environment and have verified the test cases of their modelin the a simple cloud setup[13].

Arockiam, L., &Monikandan, S. discussed reliable and flexible approach to users to store and retrieve their data at anytime and anywhere. Cloud computing is an increasingly growing technology. Nowadays, many enterprises have started using cloud storage due to its advantages. Even though the cloud continues to gain popularity in usability and attraction, the problems lie in data security, data privacy and other data protection issues. Security and privacy of data stored in the cloud are major setbacks in the field of Cloud Computing. Security and privacy are the key issues for cloud storage. This paper proposed a symmetric encryption algorithm for secure storage of cloud user data in cloud storage. The proposed encryption algorithm is described in detail and the decryption process is reverse of the encryption. This algorithm is used in order to encrypt the data of the user in the cloud[12].

Kaur, G., &Mahajan, M. analyzed the performance of security algorithms, namely, AES, DES, BLOWFISH, RSA and MD5 on single system and cloud network for different inputs. These algorithms are compared based on two parameters, namely, Mean time and Speed-up ratio[14].

Sanyal, S., & Iyer, P. proposed an algorithm which uses AES technique of 128/192/256 bit cipher key in encryption and decryption of data. AES provides high security as compared to other encryption techniques along with RSA.[15]

Reddy, V. K., & Rao, J. E. presented a couple of security solutions. Several homographic and disk encryption methods and their limitations are discussed. The efforts to combine the benefits of both the techniques give rise to further more possibilities. This study concludes that Disk encryption offers better performance, ease of development, but security is confined to disk and not the data. Homographic encryption on the other hand offers good privacy and invisibility even to the server which is encrypting the data. In this the security lies with the sharable data unit. Though homographic encryption offers better privacy, it is slow in performance and ease of development for the programmer[16].

There are many other approaches existing and been tested to make data outsourcing in Cloud computing environment bit more secure.

5. CONCLUSIONS

This paper highlighted how important it is to ensure that information within the Cloud environment is to be secure. We have discussed need of securing Cloud storage systems, challenges and basic security requirements of a Cloud computing, some of the possible threats on the Cloud Storage systems and counter measures to deal with the same. In this paper a survey of existing approaches to secure cloud computing environment and services has been expounded and discussed and found that every approach has its own pros and cons. In the future scope of this work, we will implement an approach to secure the aforesaid environment by Identity based encryption by using well known cryptographic algorithm, ECC, and the same will be evaluated and analyzed with its counterparts on appropriate simulation bed.

REFERENCES:

[1] AlZain, M. A., Pardede, E., Soh, B., & Thom, J. A. (2012). Cloud Computing Security: From Single to Multi-Clouds. 45th Hawaii International Conference on System Sciences.

[2] Sharma, B. (2013). Security Architecture of Cloud Computing Based On Elliptic Curve Cryptography (ECC). Proceedings of 2nd International Conference on Emerging Trends in Engineering and Management, Vol.3 (3).

[3] Venkataramana, K. &Padmavathamma M. (2012). A Threshold Secure Data Sharing Scheme for Federated Clouds. International Journal of Research in Computer Science, 2 (5): pp. 21-28.

[4] RajkumarBuyya, Rajiv Ranjan, and Rodrigo N. Calheiros,"InterCloud: Utility-Oriented Federation of Cloud Computing Environments for Scaling of Application Services", ICA3PP,2010,Part I, LNCS 6081, Springer, 2010, pp. 13–31. doi: 10.1007/978-3-642-13119-6_2.

[5] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications (2011), pp. 1-11. doi: 10.1016/j.jnca.2010.07.006

[6] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing", V2.1, 2009.

[7] Xiao Zhang; Hong-tao Du; Jian-quan Chen; Yi Lin; Lei-jieZeng,"Ensure Data Security in Cloud Storage", Network Computing and Information Security (NCIS), International Conference (IEEE),vol.1,14-15 May,2011 pp.284- 287. doi: 10.1109/ NCIS.2011.64

[8] Ming Li, Shucheng Yu, Yao Zheng, Wenjing Lou, "Scalable and Secure

Sharing of Personal Health Records in Cloud Computing Using Attributr based Encryption" IEEE transactions on parallel and distributed systems, Vol 24, No. 1, January 2013

[9] Jun, F., Ryo, F., Takuya, M., Kengo, M., Toshiyuki, I., &Toshinori, A. (2013). A Privacy-Protection Data Processing Solution Based on Cloud Computing. NEC Technical Journal, Vol.8 No.1.

[10] Kader, H. M. A., Hadhoud, M. M., El -Sayed, S. M. & AbdElminaam, D. S. (2014). Performance Evaluation Of New Hybrid Encryption Algorithms To Be Used For Mobile Cloud Computing. International Journal of Technology Enhancements And Emerging Engineering Research, VOL 2, ISSUE 4.

[11] Kaur, G., & Mahajan, M. (2013). Analyzing Data Security for Cloud Computing Using Cryptographic Algorithms. Int. Journal of Engineering Research and Applications, Vol. 3, Issue 5, pp.782-786.

[12] Arockiam, L., & Monikandan, S. (2013). Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm. International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue 8.

[13] Sudha, M., &Monica, M. (2012).Enhanced Security Framework to Ensure Data Security in Cloud Computing Using Cryptography. Advances in Computer Science and its Applications, Vol. 1, No. 1.

[14] Kaur, G., & Mahajan, M. (2013). Analyzing Data Security for Cloud Computing Using Cryptographic Algorithms. Int. Journal of Engineering Research and Applications, Vol. 3, Issue 5, pp.782-786.

[15] Sanyal, S., & Iyer, P. P. (2013). Cloud Computing -An Approach with Modern Cryptography. Tata Consultancy Services, Mumbai, INDIA.

[16] Reddy, V. K., & Rao, J. E. (2014). A Survey on Security in Cloud using Homographic and Disk Encryption Methods. International Journal of Computer Sciences and Engineering, Volume-2, Issue-4.