Enhancing Security in Cloud Computing: Survey

Mr. Ashish Prajapati[*], Prof.Amit Rathod[**]

[*] M.E (Computer Engineering), Parul Institiute of Engineering & Technology,
[**] Asst.Prof (IT Dept.), Parul Institiute of Engineering & Technology

Abstract- Cloud computing is everywhere. Pick up any magazine or visit almost any IT website or blog and you will be sure talk about cloud computing. There are many security issues in cloud computing like Confidentiality, Integrity and Availability (CIA). There are many techniques for provide security in cloud computing. Cloud computing performs large-scale and Complex computing. Cloud computing provide flexible solution for using users data everywhere.

Here in this paper we discuss about the types of securities and related security issues in cloud environment and also her we discuss about the security techniques to provide better solutions for enhancing security in cloud computing.

Index Terms- Cloud computing, Grid computing, Security issues, Cloud computing services, Data security.

I. INTRODUCTION

CLOUD computing has recently reached popularity and developed into a major trend in It. Cloud computing toward into IT field, Organizations and Academic point of view. Cloud computing gets its name as a metaphor for the Internet Cloud computing promises to cut operational and capital costs and more importantly, let IT department focus on strategic projects instead of keeping the datacenter running. We perform such a systematic review of cloud computing and explain the technical challenges facing in this paper. Cloud computing can be defined as utilizing the internet to provide technology enabled services to people and organization.

Cloud computing have three types. Public, Private and Hybrid. It has mainly three types of services, PaaS (Platform as a Service), SaaS (Software as a Service) & IaaS (Infrastructure as a Service). In section I, we discuss about the role of cloud computing, Importance of cloud computing, Features of cloud computing, Types and layers of cloud computing. In section II, We discuss about the security types and its challenges and some techniques to provide the solution for enhance the security. And at last section III, we discuss about the whole paper conclusion and some future scopes.

A. Features and Types of Cloud computing.

Cloud computing is emerging technique in IT and related fields. It provides flexible solution for users to use their computer in virtual world. Cloud computing word refers from the synopsis of the Grid computing, Distributed computing, Cluster computing and autonomic computing. Cloud computing provides on demand service. Figure.1 illustrations the architecture of the types of cloud computing. There are three types of cloud computing.

- Public
- Private.
- Hybrid.

In Public cloud, the whole organization can use the facility of cloud computing. Public cloud is own and it is operated by the third party. In this type of cloud the "Pay per use" model is used. All customers can share their data on same infrastructure with the limited number of configuration, Security protection and Availability alterations.

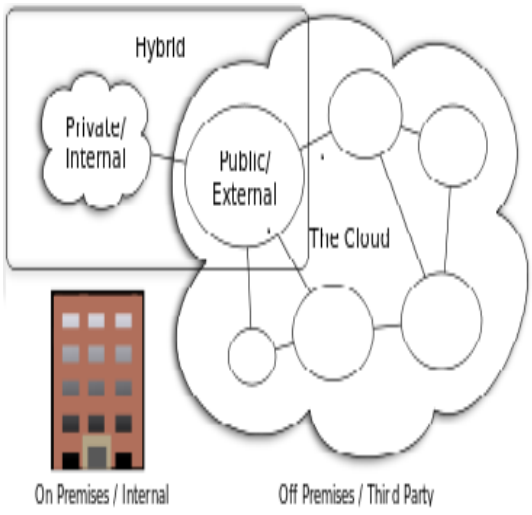

Figure 1.Types of Cloud computing.

In private cloud, the computing service is distributed for a single society. The architecture of private cloud is same as the public cloud but it is limited for a single organization.

In Hybrid cloud, the computing services is consumed both the private cloud service and public cloud service. With a Hybrid Cloud, service providers can utilize 3rd party Cloud Providers in a full or partial manner thus increasing the flexibility of computing.

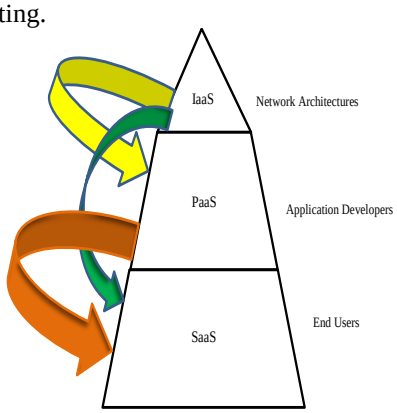

Figure 2.Architecture of Cloud Services

The basic architecture of services of cloud computing is discovered in figure 2. Cloud computing has three types of services. Software as a Service (SaaS), in which customer prepared one service and run on a single cloud, then multiple consumer can access this service as per on demand. So there is no need to purchase server or any platform. Real life example like if user wants to purchase Windows OS instead of Ubuntu, so customer contact to the cloud proprietor and pay money as per its use. Some sites work on the SaaS like Google docs, Salesforce.com, Microsoft Azure etc. Platform as a Service (PaaS), in which it provides the platform to create application and maintains the application. Examples like Google app engine, Microsoft Azure services, Force.com etc., Infrastructure as a Service (IaaS), as per term suggest to provides the data storage, Network capacity, Rent storage, Data centers etc. It is also known as Hardware as a Service (HaaS).

B. Types of Security.

Cloud computing means "Internet computing". The major problem in cloud is to provide the secure of data that is stored into the cloud environment. There are various types of security problems like Data security, Network security, Data locality, Data integrity, Authentication and etc. The central issue in cloud computing is Confidentiality, Integrity and Availability (CIA). These securities are the part of information security. Figure 3 shows the basic idea of Information security.

Confidentiality means the data stored into the cloud cannot be access by the unauthorized party. This security is prepared by applying some proper encryption techniques like symmetric key encryption or Asymmetric key encryption method, encryption techniques defends the customer's data. When customer wants to pay some bill from internet, it enters the credit card number that provides the security.

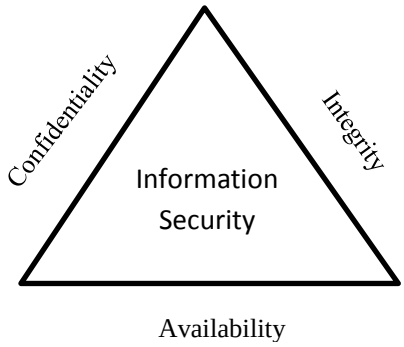

Figure 3.Basic idea of Information security.

Integrity means there is no change or modification of data when the data is transfer from source to destination. Confidentiality wills not assurance that the data has not been reformed while it exists in cloud. The data part is ensuring original till reach to the destination. Integrity is damaged when a message is actively modified in transfer.

Availability means the data should be available whenever it required. Threats targeting availability can be either network based attack such as Distributed Denial of Service (DDoS) attack.

C. Merits & Demerits of Cloud computing.

From the study of cloud computing, we studied the advantages and disadvantages. What's good? - What's the bad? – About the cloud computing, let's take a look. Here we first describe the advantages of cloud computing and then disadvantages of cloud computing. Form the merits and demerits we can studied the existing cloud technology.

- Merits of Cloud computing [20]:

1) Low Startup cost.
2) Improved performance.
3) Lower software cost.
4) Increased computing power.
5) Unlimited storage capacity.
6) Short term agreement.
7) Greater flexibility.
8) Easy to use.
9) Increased data safety.
10) Latest version available.
11) Instant software update.
12) Low infrastructure coat.

- Demerits of Cloud computing [20]:

1. Required constant internet connection.
2. Slow internet, slow performance.
3. Doesn't work with slow internet connection.
4. Features might be limited.
5. Security is not power full.
6. Stored data are not fully secured.

II. LITERATURE REVIEW

In cloud computing the major issue is to provide the security of data. Customer stores its data on cloud but the customer is not conscious about the cloud provider like the cloud provide is trusted or not. So providing security in cloud computing is the main challenge for the cloud provider. In Cloud computing data security is prepared by the Authentication, Encryption & Decryption, Message authentication code, Hash function, and Digital signature and so on. So here we discuss about some security problems and their solutions.

As per Prashant rewagad and Yogita pawar [1]: In cloud computing we have problem like to secure data storage in cloud computing. With cloud computing, organization can use the service and storage of data at any physical location outside their own control. So any unauthorized party can hack the system and use their data at any time. So in this paper, they proposed the concept of digital signature and AES encryption algorithm. Using Diffie-Hellman key exchange algorithm they first produce the key, Using this keys they authenticate the data using digital signature and at last they encrypt the data using AES encryption algorithm. The strength of their work is provide the better security in cloud computing.

As per Uma Somani, Kanika Lakhani and Manish Mundra [2]: In Cloud computing. They have anticipated a concept of digital signature with RSA algorithm, to encrypt the data while transferring it over the network. This technique solves the dual problem of authentication and security. The influence of their work is the framework proposed to address security and privacy issue.

As per Sadia marium, Qamar Nazir, Aftab Ahmed, Saira Ahthasham and Mirza Aamir Mehmood [3]: In this paper work is divided into two sections. In first section, they analyze the security problem that occurs in cloud. And In second portion, they assess the solution for providing security and confidentiality of cloud computing based on the security problem. The main role of their research is to provide the better login security in cloud computing.

As per Ashutosh dubey, Animesh dubey, Mayank namdev and Shiv Shakti Shrivastava [4]: In this paper, they proposed the framework to provide the data security in the cloud computing environment in two way secure user cloud security. They perform two tasks in it, First task is computing task and second task is admin task. They provide the security from cloud side and also from the client side. The role of this paper is providing the data security in bi directional.

Parsi Kalpana and Sudha singaraju [5] Saied that RSA encryption algorithm offers the security of confidentiality. RSA is a block cipher. It contains the public key and private key for encryption and decryption. In this paper, User data is first encrypted by using the RSA and stored into the cloud environment. When the data are required then using user's private key, user can decrypt the data without loss its originality. Major role of this solution is to provide the security of data for safe communication.

As per Pradeep bhosale, Priyanka deshmukh, Girish dimber, and Ashwini deshpande [6]: In this paper, we deliver the data security using 3D framework, Digital signature and RSA public key encryption algorithm. Using 3D framework customer can select its security level like Confidentiality; Integrity and Availability (CIA).Digital signature is the important method to authenticate the confirming user to access those data and now a day RSA public key encryption algorithm is used to provide the better security over the internet.

As per Chunming Tang, Duncan Wong, Xing Hu, Dingyi Pei. [8]: In this paper, we design a key planning scheme in cloud computing. In which two same keys are used for encryption and decryption. Without knowing the original key third party cannot break the security. It provides the secure communication. RSA algorithm is used for providing security in internet world but this key distribution method provides better security rather than RSA.

As per Mehdi Hojabri and Mona Heidari [17]: In this paper, We survey the security of cloud computing and at last we analyzed to provide the security using three parameters like RSA public key encryption algorithm, Digital signature scheme and Kerberos. In this approach, First the customer's IP will be conforming to the admin, then in second stage customer apply for taking the ticket. And at last customer can catch the cloud provider. RSA algorithm and Digital signature provide the data security in cloud environment.

As per M. Sudha and M. Monica [9]: In this paper, we proposed security framework for enhancing security in cloud computing. In this approach we proposed two step authentications, first are Login password authentication mechanism and second are digital fingerprint. Digital fingerprint mechanism enhances the security of Authentication process which is established by the

RSA public key cryptography. This mechanism prevents from the hijacking, Account attack, Password attack, Workstation hijacking of the customer's data, Denial of Service attack.

III. COCLUSION AND FUTUTRE WORK

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 that is stored into the cloud is the major problem. Security of cloud is dependent on trusted computing and cryptography.

Thus, in our survey paper, we conclude that the RSA, Digital signature and some other encryption methods provide better security over the internet. In this paper we study about the cloud computing, Types of cloud computing and Services of cloud computing. The main issue in cloud computing is to providing the security of storage data. So here we discuss about some research paper and their proposed work to providing security in cloud. As our future work we focus on reducing the security problem using some new techniques. In this we can perform DNA encryption techniques, Quantum computing techniques for providing better security.

REFERENCES

[1] Prashant Rewagad, Yogita Pawar, "Use of Digital Signature with Diffie-Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing" 2013 International Conference on Communication System and Network Technologies (IEEE Computer Society).

[2] Uma Somani, Kanika Lakhani, Manisha Mundra, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing"-2010 IEEE 1st International Conference on Parallel, Distributed and Grid Computing (PDGC-2010).

[3] Sadia marium, Qamar Nazir, Aftab Ahmed, Saira Ahthasham and Mirza Aamir Mehmood, "Implementation of Eap with RSA for Enhancing The Security of Cloud computing" International journal of Basic and Applied Science,1(3)(2012)177-183.

[4] Ashutosh dubey, Animesh dubey, Mayank namdev and Shiv Shakti Shrivastava"Cloud-User Security Based on RSA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment". Software Engineering (CONSEG), 2012 CSI Sixth International Conference on.

[5] Parsi kalpana, Sudha Singaraju "Data Security in Cloud Computing Using RSA Algorithm" International Journal of Research in Computer and Communication Technology, IJRCCT,ISSN 2278-5841, Vol.1, Issue 4, September 2012.

[6] Pradeep Bhosle, Priyanka Deshmukh, Girish Dimbar, Ashwini Deshpande" A Review Paper on Enhancing Data Security in Cloud Computing Using 3D Framework & Digital Signature with Encryption" International Journal of Engineering Research & Technology (IJERT) ISSN:2278-0181,Vol. 1 Issue 8, October – 2012.

[7] Birendra Goswami, S.N.Singh "Enhancing Security in Cloud Computing using Public Key Cryptography with Matrices" International journal of Engineering Research and Application(IJERA), ISSN:2248-9622, Vol.2, Issue 4,July-August 2012,pp.339-344.

[8] Chunming Tang, Duncan Wong, Xing Hu, Dingyi Pei "An Efficient Key Distribution Scheme in Cloud Computing" 2012 IEEE 4th International Conference on Cloud Computing Technology and Science (IEEE Computer Society).

[9] M.Sudha, M.Monica "Enhanced Security Framework to Ensure Data Security in Clod Computing Using Cryptography" Advances in Computer Science and its Applications, Vol. 1, No. 1, March 2012.

[10] Zhang jianhong, Chen Hua "Secure Storage in the Cloud Computing: A RSA-based Assumption Data Integrity Check without Original Data" 2010 International Conference on Educational and Information Technology (ICEIT 2012).

[11] Rampal Singh, Sawan Kumar, Shani Kumar Agrahari "Ensuring Data Storage Security in Cloud Computing" International Journal of Engineering And Computer Science ISSN: 2319-7242, Volume 2 Issue 3, March 2013, Page No.825-830.

[12] Dalia Attas, Omar Batrafi "Efficient Integrity Checking technique for securing Client data in Cloud Computing" International Journal of Electrical & Computer Science IJECS-IJENS Vol. 11 No: 05.

[13] Amandeep kaur, Sarpreet Singh "An Efficient Data Storage Security algorithm Using RSA algorithm" International journal of Application or Innovation in Engineering and Management (IJAIEM) Volume 2 , Issue 3, March 2013.

[14] Rajnish Choubey, Rajshree Dubey, Joy Bhattacharjee "A Survey on Cloud Computing Security, Challenges and Threats" International Journal on Computer Science and Engineering (IJCSE).

[15] Mohit Marwaha, Rajeev Bedi"Applying Encryption Algorithm for Data Security and Privacy in Cloud Computing" International Journal of Computer Science Issues (IJCSI), Vol. 10, Issue 1, No 1, January 2013.

[16] T.S.Khatri, G.B.Jethva"Survay on Data Integrity Approaches used in the Cloud Computing" International Journal of Engineering & Technology (IJERT), ISSN: 2278-0181, Vol. 1, Issue 9, November 2009.

[17] Mehdi Hojabri & Mona Heidari "Union of RSA algorithm, Digital Signature and KERBEROS in Cloud Computing" International Conference on Software Technology and Computer Engineering (STACE-2012).

[18] Mandeep Kaur, Manish Mahajan "Using Encryption Algorithm to enhance the Data Security in Cloud Computing" International Journal of Communication and Computer Technologies, Volume 1, No.12, Issue 3, January 2013.

[19] Hassan Takabi, James B.D. Joshi, Gail-Joon AHN "Security and Privacy Challenges in Cloud Computing Environment" IEEE Computer and reliability Society, 1540-7993/10/$26.00©2010 IEEE.

[20] Shivaji Mirashe, N.V.Kalyankar "Cloud Computing" Journal of Computing, Volume 2, Issue 3, March 2010, ISSN: 2151-9617.

AUTHORS

First Author- Prajapati Ashish B., M.E.(Computer Engineering)-Student, Parul Instituite of Engineering & Technology,

Second Author- Prof.Amit Rathod, Assistant Professor (Information Technology)-Guide, Parul Institute of Engineering & Technology,