A Survey on Cloud Security Threats and Solution for Secure Data in Data Stages

BL.Nithiasree*, BL.Raam Prakash**, R.Shenbaga Sundar***

Abstract:

This paper has comprehensively identified and discover vital security issues and challenges in front of cloud computing and proposed the model for cloud data security in three data stages, data-in-transit, data-in-rest, data-in-use. This paper contains four main segment, infrastructure of cloud computing, cloud security threats, vulnerability, and solution for cloud data security. First, it described the cloud service model and deployment model of cloud. Second, it explored the threats in cloud security. Third, it explored the vulnerability of cloud security. This paper has proposed the three-stage data security model in cloud computing.

Keywords--- **Cloud infrastructure Models, cloud Security Threats, Vulnerability, three-stage security of data.**

I. INTRODUCTION

CLOUD computer is using internet to deliver computer services. These includes tools and applications like data storage, servers, networking, databases, and software. Cloud Computing is considered as the first among the top ten most important technologies and with an improved prospect in successive years by companies and organizations [1]. Cloud computing offers many advantages, in that the main advantages of cloud computing is the following:

- Enhanced Flexibility.
- Rapid elasticity.
- Resource pooling.
- Improved scalability.
- Cost saving.
-

II. CLOUD INFRASTRUCTURE MODEL

The cloud services provides three layers Infrastructure models which are infrastructure as Services (IaaS), Platform as Services (PaaS) and Software as Services (SaaS) [2, 3] and provides different services.

A. Infrastructure as a Service (IaaS):

IaaS is the foundation of cloud services. This service delivers storage space, processing power and managing the organizations Database On-Demand of the particular company.

Example of IaaS vendor services includes Amazon Elastic Compute Cloud (EC2), GoGrid and Rackspace Cloud [4].

B. Platform as a Service (PaaS):

PaaS environment needed to develop the applications are delivered as a service. The organizations that need a particular environment can buy it from the cloud infrastructure for developing of their applications. This environment will run on the provider's infrastructure and release the it when the work finalized.

C. Software as a Service (SaaS):

In SaaS the software applications such as ERP and some other online applications to manage the organizations are offered as a service. Further hardware and software's that are required to support the pre made application can be offered by the cloud provider itself. Here, there is no need of investment in customer side for the service we occupy.

III. DEPLOYMENT MODEL OF CLOUD

A. Public cloud:

In this model, a CSC (Cloud service customer) uses a vendor's cloud infrastructure which is shared

publicly via the Internet with many other CSCs. This model is the most unprotected and has a change of inherent security risks that need to be measured.

B. Private cloud:

In this model, a CSC has exclusive use of cloud infrastructure and services located at the off-site, and are managed by the CSC or a CSP (Cloud service provider). This model has condensed potential security concerns compared to the public cloud.

C. Community cloud:

In this model, with related security requirement, a private cloud is shared by several CSCs. This model efforts to get most of the security benefits of a private cloud, and most of the economic benefits of a public cloud.

D. Hybrid cloud:

Hybrid Clouds are a blend of two or more cloud deployment models of resource pooling. This environment is independent and commonly connected through a standard interface [5].

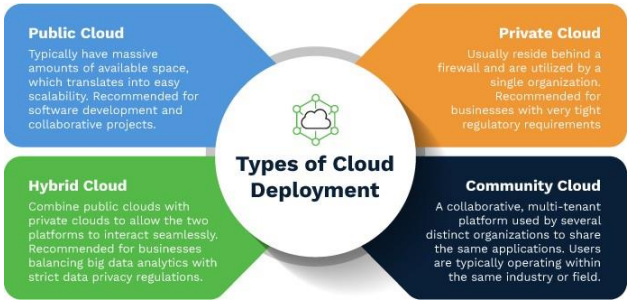

Fig.1 Deployment of Types.

IV. SECURITY THREATS

First, we introduce the basic security considerations for this deployment model followed by examine and categorize the threats specific to CSPs and CSCs.

A. Uncomplicated Security Risk:

There are a number of areas that are at risk of being compromised and hence must be secured when it comes to cloud computing. Each area represents a potential attack vector or source of failure. By risk analysis, five such key areas have been acknowledged:

1. Organizational Security Risks:

Organizational risks are categorized are categorized as the risks that may impact the structure of the organization or the business as an entity [6]. If a CSP goes out of business or gets acquired by another entity, this may negatively affect their CSPs since any Service Level Agreements (SLA) they had may have changed and they would then have to migrate to another CSP that more closely aligns with their needs.

2. Physical Security Risks:

The physical location of the cloud data center is secured by the CSP in order to prevent unauthorized on-site access of CSC data. Even encryption cannot protect against the physical theft of data. Subsequently the CSP is in charge of the physical infrastructure, they should implement and operate appropriate infrastructure controls. It is also important to note that the CSP is not only responsible for processing and sorting data in specific prerogatives but is also accountable for conforming the privacy regulations of those prerogatives.

3. Technological Security Risks:

These risks are associated with the hardware, technologies and services provided by the CSP. In the public cloud, with its multi tenancy features, these include resource sharing, and risks related to changing CSPs, i.e. portability. Here, Regular maintenance and audit of infrastructure by CSP is suggested.

4. Compliance and Audit Risks:

These are risks related to lack of prerogative information, changes in prerogative, illegal clauses in the contract and ongoing legal disputes. Data Security Risks There are a variety of data security risks that we need to take into account. The three main properties that we need to ensure are data integrity, privacy and accessibility.

B. Consideration of Data Security:

1. Privacy:

Privacy is one of the more important issues to deal with in the cloud and in network security in general. Privacy ensures that the personal information and identity of a CSC are not revealed to unauthorized users. This property is most important to the CSC, especially when they deal with sensitive data.

2. Confidentiality:

This is related to data privacy since this is the property ensuring that the data that belongs to a

CSC is not revealed to any unauthorized parties. In public clouds, the CSP is mainly responsible for securing the CSC's data. This is particularly difficult due to multi tenancy, since multiple customers have access to the same hardware that a CSC stores its data. Some providers use job scheduling and resource management, but most providers employ virtualization to maximize the use of hardware [7]. These two methods allow attackers to have full access to the host and cross-VM side channel attacks to extract information from a target VM on the same machine.

3. Integrity:

The integrity of data refers to the confidence that the data stored in the cloud is not altered in any way by unauthorized parties when it's being retrieved, i.e. you get out what you put in. To ensure this, CSPs must make sure that no third party has access to data in transit or data in storage. Only authorized CSCs should be able to change their data.

4. Availability:

This property ensures that the CSC has access to their data, and are not denied access erroneously or due to malicious attacks by any entity. Attacks like denial-of-service are typically used to deny availability of data.

***C.* Data Stages:**

The flow of data through a cloud goes through various distinct stages, with each stage requiring one or more of the previous properties to be maintained. These stages are as follows [8]:

1. Data-in-transit:

This is when through the CSC, data is in the process of being transmitted either to the cloud infrastructure or to the computing device used. Here, data is most at risk of being interrupted, hence blasphemous confidentiality. Encryption is generally used here to avert it.

2. Data-at-rest:

This is when data stored in the cloud infrastructure. The main issue in this stage is the CSC is in the loss of control over the data. The responsibility of defending against attacks at this stage henceforth fall on the CSP. CSP have to confirm that all data security properties outlined are sustained at this stage.

3. Data-in-use:

This is when data is being sort out into information. Here, the issues might take place with the corruption of data while it is being processed.

V. PROPOSED MODEL

The proposed cloud security model is composed of three layers and levels of data stages. At first, user's identification can be checked through proper authentication techniques. Security in the second layer depends on data identification and encryption. In the first level data-in -transit it uses RSA(Rivest,Shamir,Adelmen) algorithm which suits from/to web and cloud-based computing. In the second level in when the data-in-rest stage. Here, Advance Encryption Standard (AES) algorithm has been applied for the data security. At the last layer cryptography technique is used to secure the transmission of the data. The architecture of the proposed model has been shown in figure (2).

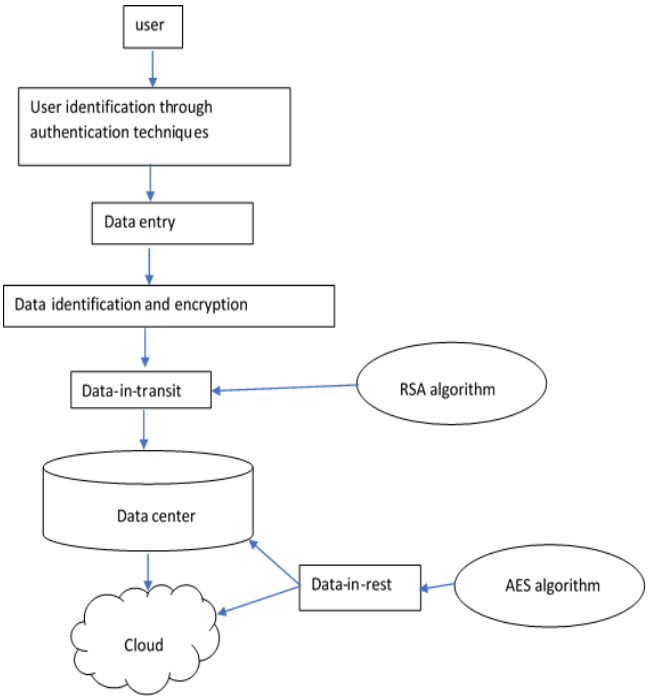

Fig.2 Proposed model.

VI. CONCLUSION

This paper proceeded to outline and examine the various security issues and vulnerability that occur in the structures used in the development of various cloud computing. First, this paper have realized that the majority of issues occur in public clouds

and relate to the security of the data that CSCs transmit to CSPs. This paper gives a survey of different threats and solutions in cloud computing environment that provides security and privacy of user's sensitive data in the cloud computing. This paper further explored on the security challenges and solutions for the cloud computing layers models and three levels of data stages. However, it remains an extremely challenging work for the future.

REFERENCE

[1] Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina, Eduardo B Fernandez, "An analysis of security issues for cloud computing", Journal of Internet Services and Applications 2013, 4:5 .

[2] Hassan Takabi , James B.D. Joshi, Gail Joon Ahn , "Cloud Computing Security and Privacy Challenges in Cloud Computing Environments ", COPUBLISHED BY THE IEEE COMPUTER AND RELIABILITY SOCIETIES,1540- 7993/10/$26.00 © 2010 IEEE.

[3] Mahesh U. Shankarwar and Ambika V. Pawar, "Security and Privacy in Cloud Computing: A Survey", Proc. of the 3rd Int. Conf. on Front. of Intell. Comput. (FICTA) 2014.

[4] Nidal Hassan and Hussein Ahmed Khalid," A survey of Cloud Computing Security challenges and solutions" International Journal of Computer Science and Information Security (IJCSIS), Vol. 14, No. 1, January 2016.

[5] S. Venkata Krishna Kumar and S.Padmapriya , "A Survey on Cloud Computing Security Threats and Vulnerabilities" , INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING Vol. 2, Issue 1, January 2014 Copyright to IJIREEICE www.ijireeice.com 622.

[6] Dahbur, K., Mohammad, B., "A Survey of Risks, Threats and Vulnerabilities in Cloud Computing.", Int Conference on Intelligent Semantic Web-Services and Applications, 2011, URL: http://www.jisajournal.com/content/4/1/5

[7] Latif, R., Abbas, H., Assar, S., Ali, Q., "Cloud computing risk assessment: a systematic literature review", Future Information Technology, pp. 285-295, Springer, Berlin, Germany, 2014., URL: http://www.researchgate.net/profile/Haider_Abbas8/publication /259221049_Cloud_Computing_Risk_Assessment_A_Systematic_Literature _Review/links /0a85e53328b478e2cb000000.pdf.

[8] Bhadauria, Rohit, Sanyal, Sugata, "Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques", Intl. Journal of Computer Applications, Vol. 47, No. 18, pp. 47-66., Foundation of Computer Science, New York, USA, URL: http://arxiv.org /pdf/1204.0764.pdf.