Review Article Impact Factor: 4.226 ISSN: 2319-507X
Rucha V. Jamnekar, IJPRET, 2015; Volume 3 (9): 1173-1178 IJPRET


INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

# SURVEY ON CLOUD COMPUTING SECURITY TECHNIQUES

**RUCHA V. JAMNEKAR[1], PROF. G. D. GULHANE[2], DR. HEMANT R. DESHMUKH[3]**

1. Student of Master of Engineering in (CSE), IBSS college of Engineering and Technology, Amravati, India.
2. Assistant professor Department of (CSE), IBSS College of Engineering and Technology, Amravati, India.
3. Head of the Department of (CSE), IBSS College of Engineering and Technology, Amravati, India.

**Accepted Date: 05/03/2015; Published Date: 01/05/2015**

**Abstract:** Cloud computing is one of the emerging technology in computer science field.it provides various services and resources. Still enterprises are disinclined to invest their business in cloud computing. It is because of security issues it has. There are different service models in cloud computing and threads to security also have different. The characteristics that are must be ensured while thinking about data security in cloud computing are integrity, availability and confidentiality.in this paper we are surveying some of the Intrusion Detecting and Prevention System and comparing then regarding their ability to provided data security. Cloud computing means that instead of all the computer hardware and software you're using sitting on your desktop, or somewhere inside your company's network, it's provided for you as a service by another company and accessed over the Internet, usually in a completely seamless way. Exactly where the hardware and software is located and how it all works doesn't matter to you, the user—it's just somewhere up in the nebulous "cloud" that the Internet represents.

**Keywords:** Cloud Security, Cloud Computing, Data Security, IDPS.

**Corresponding Author: MS. RUCHA V. JAMNEKAR**

**Access Online On:**

www.ijpret.com

**How to Cite This Article:**

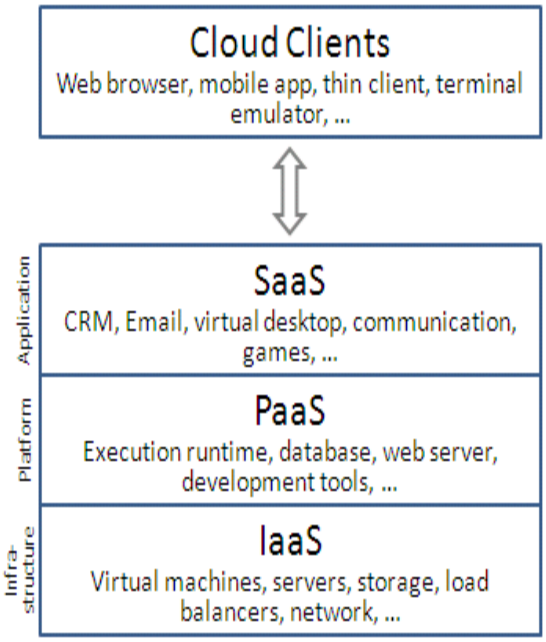
Rucha V. Jamnekar, IJPRET, 2015; Volume 3 (9): 1173-1178

***PAPER-QR CODE***

**INTRODUCTION**

Cloud Computing is a general term used to describe a new class of network based computing that takes place over the Internet, basically a step on from Utility Computing. A collection/group of integrated and networked hardware, software and Internet infrastructure (called platform).Using the Internet for communication and transport provides hardware, software and networking services to clients. These platforms hide the complexity and details of the underlying infrastructure from users and applications by providing very simple graphical interface or API (Applications Programming Interface).In addition, the platform provides on demand services that are always on anywhere, anytime and anyplace. Pay for use and as needed, elastic scale up and down in capacity and functionalities. The hardware and software services are available to general public, enterprises, corporations and businesses market. Cloud computing is an umbrella term used to refer to Internet based development and services.A number of characteristics define cloud data, applications services and infrastructure: Remotely hosted: Services or data are hosted on remote infrastructure. Ubiquitous: Services or data are available from anywhere. Commodified: The result is a utility computing model similar to traditional that of traditional utilities, like gas and electricity - you pay for what you would want!


Cloud computing providers offer their services according to several fundamental models




There are 3 cloud service models

1. Software as a Service run in your PC behind firewall (SaaS)-It provides software that run in your PC behind firewall

2. Platform as a Service (PaaS)-It provides the developmental environment as a service

3. Infrastructure as a Service (IaaS)-It will provide the infrastructure as a service.

For example server, software

Cloud computing is the future of IT but only reason for its slow growth is absence of a secure environment. In Cloud computing resources are shared. That is one of the major issues. Another thing is services are provided through a network, mainly internet. Internet is vulnerable to threats. If there are multiple users in a system we cannot assure that all of them are Following are the major characteristics of cloud computing

Trustworthy Broad network ace Elasticity and flexibility of system Shared resource pooling On demand resource allocation Shared resource pooling Pay per use services.

## II. CLOUD COMPUTING SECURITY

### 2.1 Deployment Models

There are three deployment models for cloud cc are Public Cloud, Private Cloud and Hybrid Cloud mainly. Features of each deployment models are described below problem with this type of deployment is not at all secured for them. Client will not be aware about the infrastructure. The provider serves multiple clients and provide the infrastructure provided by the cloud service provider. These cloud service Each client has his/her own resources that are In Public cloud, customers will access services over the web.

#### 2.1.1 Public Cloud

In Public cloud, customers will access services over the web. Each client has his/her own resources that are provided by the cloud service provider. These cloud service provider serves multiple clients and provide the infrastructure for them. Client will not be aware about the infrastructure. The problem with this type of deployment is not at all secure.

#### 2.1.2 Private Cloud

In private cloud client is managing their data. Client will decide where the data should reside and what level of security is needed. Also the data is more secured assuming that all the users are trusted.

#### 2.1.3 Hybrid Cloud

Hybrid Cloud is mixture of public and private cloud within the same network. Clients can store sensitive data on their private cloud and use the public cloud for storing high volume of data

### 2.2 Different Types of Threats

To provide secure environment for cloud computing should ensure confidentiality and integrity. Confidentiality means the data should not be available to any user who is not authorized. By providing integrity we are ensuring that data will not change or delete by a unauthorized user. Types of threats in cloud computing is given below.

| Threat | Description |
|---|---|
| **Malicious Insiders** | Cloud service provider misuse the user's data or resource |
| **Man in the Middle attacks** | Third party tries to access the data in Third party tries to access |

| | |
|---|---|
| | the data in transmit or inject the faulty data |
| **Denial of Service Attacks** | Denying the services to authorized user |
| **Data Loss** | Deleting or updating the sensitive data in unauthorized way |

**2.3 Detection Methodologies**

Various threat detection methodologies are there. We can categorize them depending on the methodology used. First is signature based threat detection. In this methodology they will monitor behavior of the client and if known pattern of unauthorized behavior is found take it as threat. But it will not detect the new attacks which are not defined yet. Next is anomaly detection, in which any unexpected behavior is taken as a threat and it will help to find out the new attacks. But the number of false alarms may be high comparing with the signature based threat detection methodology. Another broad category is hybrid threat detection methodology. Here uses the combination of the signature based detection methodology and anomaly detection methodology.

**2.4 Different Detection Techniques**

Juels et al. (2007) proposed a POR (Proof of Retrievability) model to check whether the file to be retrieved is correct or not. POR has a Cryptographic sum and in this technique needed to check this cryptographic sum to verify the integrity of the data. This checksum does not depend on the size of the file. One advantage of using this technique is the user can check the integrity without downloading the file. Author proposed this particular technique for large files. Shacham and Waters (2008) built on this model and constructed a random linear function based Homomorphic Authenticator. The central challenge is, it should be possible to extract the user's data from cloud service provider that passes a verification check. In this paper, gives the first proof-of retrievability schemes with full proofs of security against arbitrary adversaries in the strongest model, that of Juels and Kaliski. First scheme, based on BLS signatures, has the shortest query and response of any proof-of-retrievability with public verifiability. Second scheme, which is based on pseudorandom functions, has the shortest response of any proof-of retrievability scheme with private verifiability. Bowers et al. (2008a) proposes a theoretical framework for the design of PORs. It improves the previously proposed POR constructions of Juels-Kaliski and Shacham-Waters. It supports a fully Byzantine adversarial model, possessing only the restriction- fundamental to all PORs-that the adversary's error rate be bounded when the client seeks to extract F. This techniques support efficient protocols across the full possible range of Ɛ, up to non-negligibly close to 1. Proposes a new variant on the Juels-Kaliski protocol. Bowers et al.(2008b) introduced HAIL (High-Availability and Integrity Layer). It is a distributed

cryptographic system that allows a set of servers to prove to a client the integrity of a file. Proofs in HAIL are efficiently computable by servers and highly compact. HAIL cryptographically verifies and reactively reallocates file shares.

**III.CONCLUSIONS**

This paper presented a comparative study on some threats and threat detection techniques used in cloud computing. Specific concentration given to the threat detection techniques. In the future, we plan to develop threat detection technique which is based on these concepts and their advantages.

**IV.REFERENCES**

1. Bowers KD, Juels A, Oprea A. Proofs of retrievability: theory and implementation, Cryptology e-Print Archive.

2. Bowers KD, Juels A, Oprea A. HAIL: a high-availability and integrity layer for cloud storage, Cryptology e-Print

3. Juels A, Burton J, Kaliski S. PORs: proofs of retrievability for large files.

4. Kamara S, Lauter K. Cryptographic cloud storage.

5. Shacham H, Waters B. Compact Proofs of Retrievability.

6. Hassan, Qusay (2011). "Demystifying Cloud Computing". The Journal of Defense Software Engineering (CrossTalk) 2011 (Jan/Feb): 16–21. Retrieved11 December 2014.

7. "The NIST Definition of Cloud Computing". National Institute of Standards and Technology. Retrieved 24 July 2011.

8. "Know Why Cloud Computing Technology is the New Revolution". By Fonebell. Retrieved 8 January 2015.

9. "What is Cloud Computing?". Amazon Web Services. 2013-03-19. Retrieved 2013-03-20.

10. Oestreich, Ken, (2010-11-15). "Converged Infrastructure". CTO Forum. Thectoforum.com. Retrieved2011-12-02.