An Overview of Cloud Computing and Security Issues

Monal R. Sharma, S. S. Asole

Abstract: Cloud computing is a kind of Internet-based computing that provides shared processing resources and data to computers and other devices on demand. Security in Cloud computing is an important and critical aspect, and has numerous issues and problem related to it. Cloud service provider and the cloud service consumer should make sure that the cloud is safe enough from all the external threats so that the customer does not face any problem such as loss of data or data theft. This paper presents a review on the cloud computing concepts as well as security issues inherent within the context of cloud computing and cloud infrastructure.

Keyword: cloud computing, security issues, SaaS, PaaS, LaaS,

I. INTRODUCTION

Cloud Computing is essentially an extreme form of outsourcing in the delivery of hosted services via the internet. The cloud acts as a virtual server that users canacess via the internet on an as needed basis. Cloud computing includes any subscription-based or pay-per-use service that extends IT capabilities allowing users to acess their stored information remotely. Cloud computing is the latest effort in delivering computing resources as a service. It represents a shift away from computing as a product that is purchased, to computing as a service that is delivered to consumers over the internet from large-scale data centres – or "clouds**".** Cloud computing is an architecture for providing computing pay per use access to a pool of shared resources namely networks, storage, servers, services and applications, without physically acquiring them. So it saves managing cost and time for organizations. Many industries, such as banking, healthcare and education are moving towards the cloud due to the efficiency of services provided by the pay-per-usepattern. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. This technology allows for much more efficient computing by centralizing storage, memory, processing and bandwidth.

II. LITERATURE SURVEY

M.B. Mollah, Kazi ReazulIslam, Sikder Sunbeam Islam "Next Generation of Computing through Cloud Computing Technology"[1]. In this paper presents all about of cloud computing which is a new emerging technology in present world. Although there are several issues and challenges in cloud computing technology, a huge scope for research and we can say that it is a development trend in near future.Prince Jain "Security Issues and their Solution in Cloud Computing"[2].This paper firstly lists the parameters that affect thesecurity of the cloud then it explores the cloud security issues and problems faced by cloud service provider and cloud service consumer such as data, privacy, and infected application and security issues. It also discuses some tips for tackling these issues and problems.Rabi Prasad Padhy, ManasRanjanPatra, Suresh Chandra Satapathy "Cloud Computing: Security Issues and Research Challenges"[3].This research paper also analyzes the key research and challenges that presents in cloud computing and offers best practices to service providers as well as enterprises hoping to leverage cloud service to improve their bottom line in this severe economic climate.Monjur Ahmed and Mohammad Ashraf Hossain "Cloud Computing and security issues in cloud"[4].This paper presents a review on the cloud computing concepts as well as security issues inherent within the context of cloud computing and cloud infrastructure. Pankaj Arora, Rubal Chaudhry Wadhawan, Er. Satinder Pal Ahuja "Cloud Computing Security Issues in Infrastructure as a Service"[5].This paper presents an elaborated study of IaaS components' security and determines vulnerabilities and countermeasures. Service Level Agreement should be Considered very much importance. MohsinNazir "Cloud Computing: Overview & Current Research Challenges"[6].7)Vahid Ashktorab, Seyed Reza Taghizadeh "Security Threats and Countermeasures in Cloud Computing"[7].In this paper, we have cast light over the major security threats of cloud computing systems, while introducing the most suitable countermeasures for them. We have also cited the aspect to be focused on when talking about cloud security. We have categorized these threats according to different viewpoints, providing a useful and little-known list of threats. After that some effective countermeasures are listed and explained. Abhishek Goel, Shikha Goel "Security Issues in Cloud Computing"[8].In this paper security in cloudcomputing is elaborated in a way that covers security issues, concerns and challenges for Data Security in Cloud. Threats to cloud confidentiality, cloud integrity, cloud availability& cloud privacy and related issues are discussed in this paper.9) Pradeep Kumar Tiwari, Dr. Bharat Mishra "Cloud Computing Security Issues, Challenges and Solution"[9].This paper also cover the advantages and disadvantages in the way of cloud computing.

Revised Version Manuscript Received on July 30, 2016.

Ms. Monal R. Sharma, M.E. First Year, Department of Computer Science & Engineering, Babasaheb Naik College of Engineering, Pusad, Yavatmal (Maharashtra). India.

S. S. Asole, Associate Professor, Department of Computer Science & Engineering, Babasaheb Naik College of Engineering, Pusad, Yavatmal (Maharashtra). India.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

This paper also tackles the important aspect of security concerned challenges which the researchers and authors are facing in the security of cloud computing.10)Nir Kshetri “Privary and security issues in cloud computing”[10].In this paper investigate how the contexts provided by formal and informal institutions affect privacy and security issues in the cloud.

III. OVERVIEW

Cloud computing is the delivery of computing services over the Internet. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. Examples of cloud services include online file storage, social networking sites, webmail, and online business applications. The cloud computing model allows access to information and computer resources from anywhere that a network connection is available. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications. Cloud computing refers to the delivery of computing resources over the Internet. Instead of keeping data on your own hard drive or updating applications for your needs, you use a service over the Internet, at another location, to store your information or use its applications. Doing so may give rise to certain privacy implications.

A. Why Cloud Services are Popular

Cloud services are popular because they can reduce the cost and complexity of owning and operating computers and networks. Since cloud users do not have to invest in information technology infrastructure, purchase hardware, or buy software licences, the benefits are low up-front costs, rapid return on investment, rapid deployment, customization, flexible use, and solutions that can make use of new innovations. In addition, cloud providers that have specialized in a particular area (such as e-mail) can bring advanced services that a single company might not be able to afford or develop. Some other benefits to users include scalability, reliability, and efficiency. Scalability means that cloud computing offers unlimited processing and storage capacity. The cloud is reliable in that it enables access to applications and documents anywhere in the world via the Internet. Cloud computing is often considered efficient because it allows organizations to free up resources to focus on innovation and product development.

IV. CHARACTERISTICS

- **Agility:** Agility improves with users' ability to re-provision technological infrastructure resources.
- **Cost:** Cost reductions claimed by cloud providers. A public-cloud delivery model converts capital expenditure to operational expenditure. This purportedly lowers barriers to entry, as infrastructure is typically provided by a third party and need not be purchased for one-time infrequent intensive computing tasks. Pricing on a utility computing basis is fine-grained, with usage-based options and fewer IT skills are required for implementation.
- **Device and location independence:** independence enable users to access systems using a web browser regardless of their location or what device they use .As infrastructure is off-site and accessed via the Internet, users can connect from anywhere.
- **Maintenance:** Maintenance of cloud computing applications is easier, because they do not need to be installed on each user's computer and can be accessed from different places.
- **Performance:** Performance is monitored and consistent and loosely coupled architectures are constructed using web services as the system interface.
- **Productivity:** Productivity may be increased when multiple users can work on the same data simultaneously, rather than waiting for it to be saved and emailed.
- **Reliability:** Reliability improves with the use of multiple redundant sites, which makes well-designed cloud computing suitable for business continuity and disaster recovery.
- **Security:** Security can improve due to centralization of data, increased security-focused resources, etc., but concerns can persist about loss of control over certain sensitive data, and the lack of security for stored kernels. Security is often as good as or better than other traditional systems, in part because providers are able to devote resources to solving security issues that many customers cannot afford to tackle. However, the complexity of security is greatly increased when data is distributed over a wider area or over a greater number of devices, as well as in multi-tenant systems shared by unrelated users. In addition, user access to security audit logs may be difficult or impossible. Private cloud installations are in part motivated by users' desire to retain control over the infrastructure and avoid losing control of information security.

V. TYPES OF CLOUD COMPUTING

Cloud computing is typically classified in two ways:

- **Location of the cloud computing**
- **Types of services offered**
- **Location of the cloud computing :**

Cloud computing is typically classified in the following three ways:

1) **Public cloud:** In Public cloud the computing infrastructure is hosted by the cloud vendor at the vendorâ€™s premises. The customer has no visibility and control over where the computing infrastructure is hosted. The computing infrastructure is shared between any organizations.
2) **Private cloud:** The computing infrastructure is dedicated to a particular organization and not shared with other organizations. Some experts consider that private clouds are not real examples of cloud computing. Private clouds are more expensive and more secure when compared to public clouds.

3) **Hybrid cloud:** Hybrid cloud organizations may host critical applications on private clouds and applications with relatively less security concerns on the public cloud. The usage of both private and public clouds together is called hybrid cloud. A related term is Cloud Bursting. In Cloud bursting organization use their own computing infrastructure for normal usage, but access the cloud using services like Sales force cloud computing for high/peak load requirements. This ensures that a sudden increase in computing requirement is handled gracefully.

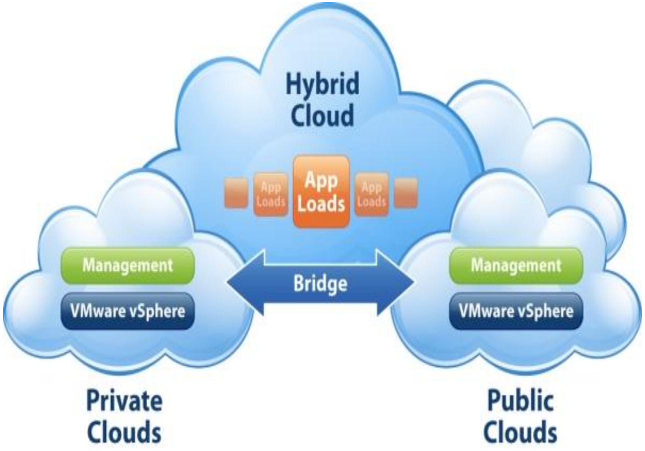

Fig1. Location of cloud computing

A. Types of services offered :

The service-oriented architecture advocates "everything as a service "cloud-computing providers offer their "services" according to different models, of which the three standard models per NIST are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).These models offer increasing abstraction; they are thus often portrayed as a layers in a stack: infrastructure platform- and software-as-a-service,but these need not be related. For example, one can provide SaaS implemented on physical machines (bare metal), without using underlying PaaS or IaaS layers, and conversely one can run a program on IaaS and access it directly, without wrapping it as SaaS.

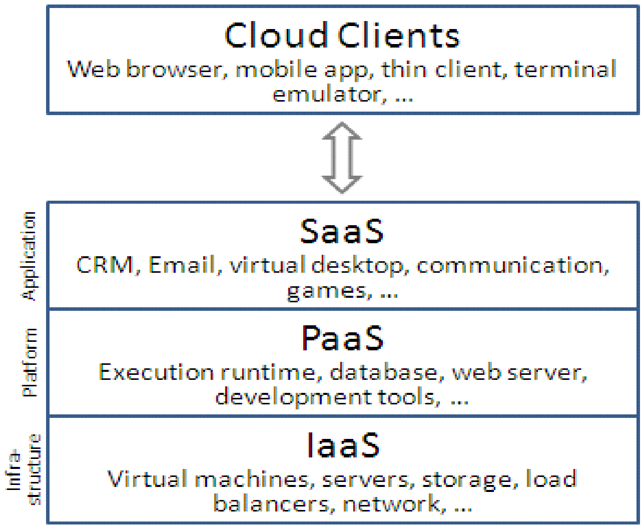
Cloud Clients
Web browser, mobile app, thin client, terminal emulator, ...
Application
SaaS
CRM, Email, virtual desktop, communication, games, ...
Platform
PaaS
Execution runtime, database, web server, development tools, ...
Infra-structure
IaaS
Virtual machines, servers, storage, load balancers, network, ...

Fig2. Types of Services

- **Software as a Service (SaaS):** The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
- **Platform as a Service (PaaS):** The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
- **Infrastructure as a Service (IaaS):** The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components.

VI. ADVANTAGES

1) Worldwide Access
2) More Storage
3) Easy Set-Up
4) Automatic Updates
5) Reduced Cost

VII. DISADVATEGES

1) Security
2) Privacy
3) Loss of Control
4) Internet Reliance
5) Limited Control
6) Cost and time transferring data across the cloud

VIII. CLOUD COMPUTING SECURITY ISSUES

A. Parameters affecting cloud security

There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management Security issues for many of these systems and technologies are applicable to cloud computing.

*Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.*

B. Security Issues faced by Cloud computing

Whenever a discussion about cloud security is taken place there will be very much to do for it. The cloud service provider for cloud makes sure that the customer does not face any problem such as loss of data or data theft. There is also a possibility where a malicious user can penetrate the cloud by impersonating a legitimate user, there by infecting the entire cloud. This leads to affects many customers who are sharing the infected cloud. There are four types of issues raise while discussing security of a cloud.

1) Data Issues
2) Privacy issues
3) Infected Application
4) Security issues

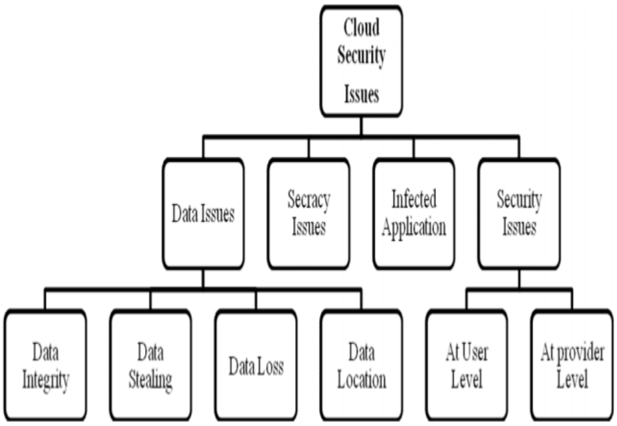

Fig.3. Security Issues in Cloud Computing

1) Data Issues:

Sensitive data in a cloud computing environment emerge as major issues with regard to security in a cloud based system. Firstly, whenever a data is on a cloud, anyone from anywhere anytime can access data from the cloud since data may be common, private and sensitive data in a cloud. So at the same time, many cloud computing service consumer and provider accesses and modify data.

2) Secrecy Issues:

The cloud computing service provider must make sure that the customer personal information is well secured from other providers, customer and user. As most of the servers are external, the cloud service provider should make sure who is accessing the data and who is maintaining the server so that it enable the provider to protect the customer's personal information.

3) Infected Application:

Cloud computing service provider should have the complete access tothe server with all rights for the purpose of monitoring and maintenance of server. So this will prevent any malicious user from uploading any infected application onto the cloud which will severely affect the customer and cloud computing service.

4) Security issues:

Cloud computing security must be done on two levels. One is on provider level and another is on user level. Cloud computing service provider should make sure that the server is well secured from all the external threats it may come across. Even though the cloud computing service provider has provided a good security layer for the customer and user, the user should make sure that there should not be any loss of data or stealing or tampering of data for other users who are using the same cloud due to its action. A cloud is good only when there is a good security provided by the service provider to the user.

IX. CONCLUSION

Every new technology has its pros and cons, similar is the case with cloud computing. Although cloud computing provides easy data storage and access. But there are several issues related to storing and managing data, that is not controlled by owner of the data. This paper discuss about Various Layers of Infrastructure as a Service. In this paper we also discuss characteristics, advantages and disadvantages of cloud computing. This paper also discussed security issues for cloud. These issues include cloud integrity, cloud confidentiality, cloud availability, cloud privacy.

ACKNOWLEDGMENT

I would like to thank my supervisor and all of my teachers for their helpful comments in improving our manuscript.

REFERENCE

1. Muhammad Baqer Mollah, Kazi Reazul Islam*, Sikder Sunbeam Islam "Next Generation of Computing through Cloud Computing Technology"
2. Prince Jain "Security Issues and their Solution in Cloud Computing"
3. Rabi Prasad Padhy, Manas Ranjan Patra, Suresh Chandra Satapathy "Cloud Computing: Security Issues and Research Challenges"
4. Monjur Ahmed and Mohammad Ashraf Hossain "Cloud Computing and security issues in cloud"
5. Pankaj Arora, Rubal Chaudhry Wadhawan, Er. Satinder Pal Ahuja "Cloud Computing Security Issues in Infrastructure as a Service"
6. MohsinNazir "Cloud Computing: Overview & Current Research Challenges"
7. VahidAshktorab, Seyed Reza Taghizadeh "Security Threats and Countermeasures inCloud Computing"
8. Abhishek Goel, ShikhaGoel "Security Issues in Cloud Computing"
9. Pradeep Kumar Tiwari, Dr. Bharat Mishra "Cloud Computing Security Issues, Challenges and Solution"
10. NirKshetri "Privary and security issues in cloud computing"