



ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirccce.com

Vol. 5, Issue 9, September 2017

A Study on Security Aspects of Grid and Cloud Computing

Dr. Ranjit D. Patil¹, Sujata P. Patil², Vidya H. Bankar³

Assistant Professor, Dept. of Computer Science, Dr. D. Y. Patil A.C.S College, Pimpri, Pune, India¹.

Assistant Professor, Dept. of Computer Science, Dr. D. Y. Patil A.C.S College, Pimpri, Pune, India².

Assistant Professor, Dept. of Computer Science, Dr. D. Y. Patil A.C.S College, Pimpri, Pune, India³.

ABSTRACT: Cloud Computing provides us means by which we can access the applications as services over the internet. It allows users to create, configure, and customize the business applications online at anytime and anywhere without worrying about location. Cloud computing offers platform independency, as the software is not required to be installed locally on the PC.

Grid computing provides high computing power, huge data storage, and collaboration possibilities to its users.

Several challenges however still hamper both the technology, and resolving security problems with grid computing and cloud computing is one such major challenge.

This paper describes overview of different security issues in Cloud and Grid Computing and also suggested some security measures for protecting personal data of individuals and organizations from malicious intruders.

KEYWORDS: Cloud Computing, Grid Computing, Public Cloud, Security.

I. INTRODUCTION

Cloud is a popular computer term refers to a Network or Internet. Cloud computing means on demand delivery of IT resources via the internet with pay-as-you-go approach. It provides a solution of IT infrastructure in low cost. The cloud is usually opaque to the end user as the end user does not have to manage the core technology.

A cloud refers to a distinct IT environment that is designed for the purpose of remotely provisioning scalable and measured IT resources. The term originated as a metaphor for the Internet which is, a network of networks providing remote access to a set of decentralized IT resources and services.

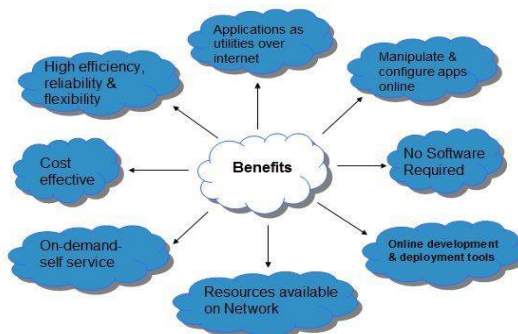


Figure1: Cloud Computing Benefits

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

II. RELATED WORK

In the last few years, Cloud and Grid computing has grown from being a promising business concept to one of the fast-growing segments of the IT industry. But as more and more information on individuals and companies are placed in the cloud, concerns are beginning to grow about just how safe an environment. A number of vulnerabilities and threats focused in Cloud Computing and Grid Computing. The studies analyze the risks and threats, often give recommendations on how they can be avoided or covered. In addition, we can see that in our search, many of the approaches, in addition to speaking about threats and vulnerabilities, also discuss other issues related to security in the Cloud such as the data security, trust, or security recommendations and mechanisms for any of the problems encountered in these environments.

III. DEPLOYMENT MODELS IN CLOUD COMPUTING

1. **Public Cloud:** A public cloud is one based on the standard cloud computing model, in which a service provider makes resources, such as virtual machines (VMs), applications or storage, available to the general public over the internet. Public cloud services may be free or offered on a pay-per-usage approach. It also reduces the need for organizations to invest in and maintain their own on-premises IT resources.
2. **Private Cloud:** Private cloud is a type of cloud computing that delivers similar advantages to public cloud, including scalability and self-service, but through a proprietary architecture. Unlike public clouds, which deliver services to multiple organizations, a private cloud is dedicated to a single organization
3. **Hybrid Cloud:** The cloud infrastructure consists of multiple clouds of any type, but the clouds have the ability through their interfaces to allow data and/or applications to be moved from one cloud to another. This can be a combination of private and public clouds.
4. **Community Cloud:** The cloud infrastructure is shared among a number of organizations with similar interests, policies and requirements.

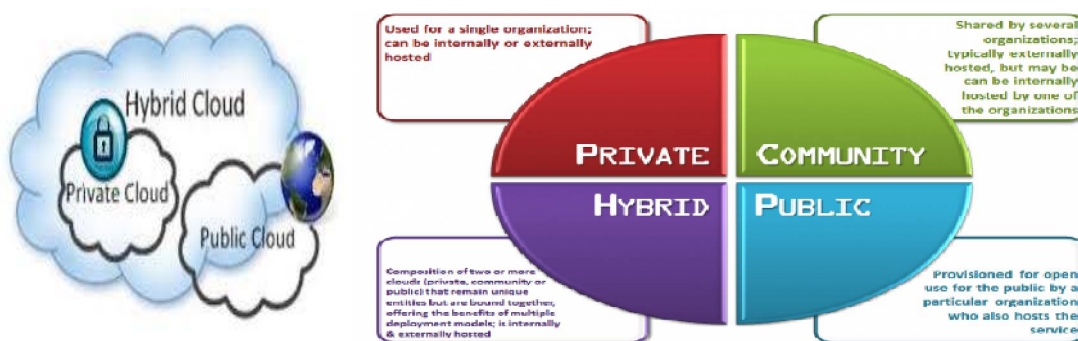


Figure 2: Deployment Model in Cloud Computing

There are three service models in cloud computing as **Software-as-a-Service (SaaS)**, **Platform-as-a-Service (PaaS)** and **Infrastructure-as-a-Service (IaaS)**:

- **Infrastructure-as-a-Service (IaaS):** Raw or fundamental computing resources like virtual computers, servers, storage devices and network transfer are physically located in one central place (data center) but they can be accessed and used over the internet using the login authentication systems. It is also called as Hardware-as-a-Service (HaaS).



ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

- **Platform-as-a-Service (PaaS):** Instead of buying the software licenses for platforms like operating systems and databases, these platforms and the software development kits and tools (like Java, .NET) are made available over the Internet. It is the middle bridge between hardware and application.
- **Software-as-a-Service (SaaS):** Instead of installing special software on your computer and updating it with regular patches, frequent version upgrades etc., applications like Word processing, Customer Relationship Management, Enterprise Resource Planning are made available over the internet for the consumption of the customer.

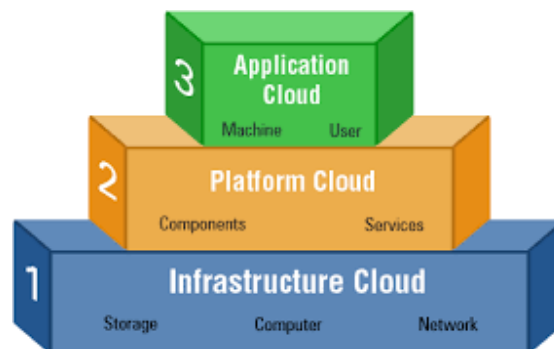


Figure 3: Service models in cloud computing

IV. CLOUD COMPUTING CHALLENGES

Cloud Computing is the important innovation happening in the field of Information Technology. This technology utilizes internet to provide technology enabled services to individuals and organization. In spite of its growing influence, security concerns regarding cloud computing still remains.

The increase in growth of cloud computing brought lots of security issues/challenges for customers and service providers.

Following are some major challenges of cloud computing while its implementation.

1. Phishing Attacks:

Due to the openness of a cloud computing system, phishing attacks have become particularly common. Once login information or other confidential information is acquired, a malicious user can possibly break into a system with ease because the system itself is available from anywhere.

2. Application security:

SaaS provides application services on demand such as email, conferencing software, and business applications. SaaS users have less control over security. The applications are typically delivered via the Internet through a Web browser. However, faults in web applications may create vulnerabilities for the SaaS applications. Attackers have been using the web to compromise user's computers and perform malicious activities such as steal sensitive data.



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

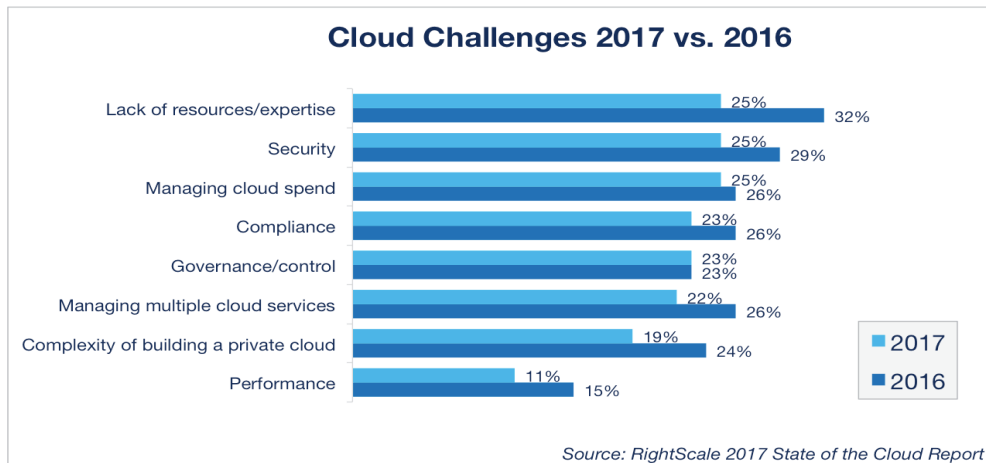


Figure 4: Graphical Presentation on Cloud Computing Challenges

3. Data Security and Privacy:

Data protection is among the biggest concerns in cloud computing. A number of security threats are associated with cloud data services are network eavesdropping, illegal attack, and denial of service attacks. When confidential information is hosted by cloud service providers on the internet, it means that a considerable amount of the end user's security and privacy control is transferred to the cloud vendor. It is essential to ensure the cloud provider understands the end user's security and privacy needs, which normally presents the big challenge.

4. Accessibility:

Accessing applications over the internet via web browser makes access from any network device easier, including public computers and mobile devices. However, it also exposes the service to additional security risks.

5. Distributed Denial of Service Attack (DDoS):

This attack is the form of attack that an attacker aims to prevent valid users from accessing information or services. The common type of this attack occurs when an attacker floods a network with excessive requests to the target server until the server is unable to provide services to normal users.

6. Governance/Control: Governance means keeping control and oversight over policies, procedures and standards for application development.

7. Legal issues: Geographical locations are not fixed for any resources in the clouds. They may migrate between the physical locations due to different factors and reasons. Because of migration they may come under multiple legal jurisdictions and these may have some conflicting rules about security issues such as intrusion and data protection.

8. Integrity: Integrity means modifications of data, referring of data, software and hardware. Integrity can be done only by authorized parties and in authorized way. Integrity is a key aspect of security in cloud computing. It is also related to data stolen and data loss.

Some of the Solutions for Cloud Computing Security Issues:

1. Secure stored data. Data should be securely encrypted when it's on the provider's servers and while it's in use by the cloud service.
2. Confidential information is shared with an outside party and thus, it's always advisable for cloud computing users to ensure that their providers are aware of certain data security and privacy rules and regulations.



ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

3. The Cloud Security Alliance (CSA) recommends that users should be aware of the software interfaces that are used to interact with cloud services.
Trust on a weak set of interfaces exposes organizations to a variety of security issues related to confidentiality, integrity, availability, and accountability.
4. Sensitive data stored into the cloud. Some researcher suggested that ask providers for specifics about the people who manage data and the level of access they have to it.
5. Secure Data Transfer is one more essential factor. All of the traffic travelling between network and whatever service users accessing in the cloud must traverse the through Internet. Make sure users data is always travelling on a secure channel; only connect your browser to the provider via a URL that begins with “https”.
6. For legal issues migration rules, country location restrictions are defined and enforced in service level agreement. Providers should assure customers that their data is safe, authentic. Legal issues are not attacks but they might violate security goals.
7. Governance problem can be solved by including security metrics and standards in service level agreements.
8. Employees must be knowledgeable about phishing enough to avoid these types of attacks.

V. GRID COMPUTING

Grid computing is a utility for complex huge computations, where remote resources are accessible through web. It is a computer network in which computer's resources (Processing power, memory and data storage) are shared with every other computer in the system. The grid computing is a special kind of distributed computing. It allows widely dispersed organizations and businesses to create virtual organizations to share data and resources.

A Grid is basically the one that uses the processing capabilities of different computing units for processing a single task without increasing cost and by reducing time taken to complete task. Computers on a grid are not necessarily in the same geographical location, and can be spread out over multiple countries and organizations.



Figure 5: Grid Computing



ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

VI. SECURITY ISSUES IN GRID COMPUTING

The goal of Grid Computing is to provide secure grid service resources to legal users and therefore security issues become an important concern of grid computing.

There are major security risks in every application downloaded from internet. Whenever two or more computers are linked together there is risk protecting computer or data from malicious attacks. Personal information or data not remains secure. We cannot control who can access the system and its resources.

1. Grid should protect flow of information to trusted parties.
2. User's Data should be protected.
3. User's personal data and system data should be distinguished.
4. Resource level authorization.
5. Delegation of Identity.

Some of the Solutions for Security issues in Grid:

- The Security in Grid environment is achieved through the implementation of various security measures such as authentication, authorization and security of data.
- Authentication should be done each time when user enters in a grid.
- Authentication or verifying identity of the participant. Traditional systems authenticate clients to protect the server, grid systems require mutual authentication to ensure protection against attackers.
- Password should be encrypted.
- Authorization uses such process which identifies which operation is allowed for particular user.
- Network activity should be continuously monitored.
- In grid computing security of data is high, it must be ensuring that integrity and confidentiality of the data being transmitted over the network. Some of the techniques are used for creating securing grids, such as Symmetric Key Cryptography and Asymmetric Key Cryptography.
- Monitoring resource usage.
- Single sign on or delegation capacity, to reduce the number of times a user needs to enter password.

VII. CONCLUSION

Cloud and Grid Computing is a relatively new concept that presents a several benefits for individuals as well as organizations. But it also raises some security problems which may slow down its use and due to this issue people are hesitating to use the clouds. To realize benefits of Cloud and Grid users must have assurance about security of privacy of their personal data. In this paper, we have discussed various security issues of cloud computing and Grid Computing. We have also recommended some security measures that will definitely help organizations and users to protect their data from malicious attackers. Also, some strong authentication procedures must be developed in future for the sake of security of resources in the grid and cloud environment.

REFERENCES

1. http://whatiscloud.com/basic_concepts_and_terminology/cloud
2. <https://blog.econocom.com/en/blog/why-companies-are-adopting-hybrid-cloud/>
3. <http://www.brighthub.com/environment/green-computing/articles/94587.aspx>



ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

4. Ms. Vaishali R. Wadhe, Dr. Vinayak A. Bharadi International Journal of Scientific & Engineering Research, Volume 5, Issue 1, January 2014 106 ISSN 2229-5518 IJSER Security Aspect of Cloud Computing
5. <http://www.sciencedirect.com/science/article/pii/S0167739X10002554>
6. https://en.wikipedia.org/wiki/Cloud_computing
7. https://en.wikipedia.org/wiki/Grid_computing
8. <https://www.cs.clemson.edu/course/cpsc420/.../Grid%20Computing%20Security.ppt>
9. <https://jisajournal.springeropen.com/articles/10.1186/1869-0238-4-5>

BIOGRAPHY

Dr. Ranjit D. Patil is Vice Principal and H.O.D. (Computer Science Department), Dr. D. Y. Patil Arts, Commerce and Science College Pimpri, Savitribai Phule Pune University. He received M.C. S degree in 2000 and Ph.D. degree in 2013 from Savitribai Phule Pune University, MS, India. He has cleared the NET Examination held by UGC in 2006. He has also received M.Phil. (Computer Science) degree in 2013 from Alagappa University, Tamilnadu, India. His research interests are E-Commerce, Information Security and Information Technology etc.

Ms. Sujata P. Patil is an Assistant Professor in the Computer Science Department, Dr. D. Y. Patil Arts, Commerce and Science College Pimpri, Savitribai Phule Pune University. She received M.C.S degree in 2004 from Savitribai Phule Pune University, MS, India and M.Phil. (Computer Science) degree in 2010 from Alagappa University, Tamilnadu, India. Her research interests are E-Commerce, Information Security etc.

Ms. Vidya H. Bankar is an Assistant Professor in the Computer Science Department, Dr. D. Y. Patil Arts, Commerce and Science College Pimpri, Savitribai Phule Pune University. She received M.Sc. Computer Science degree in 2009 from Savitribai Phule Pune University, MS, India. Her research interests are E-Commerce, Information Security etc.