SCHOLEDGE INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY & ALLIED STUDIES
VOL. 1, ISSUE 2(NOVEMBER 2014) ISSN-2394-336X

CLOUD COMPUTING-AN IMPLEMENTATIONAL STORYLINE OF COMPUTING

GUNNAR KNAUS,
Guest Faculty,
GRAZ, AUSTRIA.

ABSTRACT

Cloud computing today is the latest catchphrase in the software industry. Although Cloud computing has achieved a great success in various industries whether it be a software industry, a Government Organization or a Healthcare sector, but this transition to Cloud computing has fuelled concerns on a critical issue for the success of information systems, communication and information security. Form the viewpoint of security, various risks and issues are identified in the area of Cloud Computing. There are various risks associated with the security but one of the major issues is the security of data being stored on the provider's cloud and privacy while the data is being transmitted. This paper deals with various issues associated with Security and focus mainly on the data security and methods of providing security by Cryptology Algorithm.

Key Words: Cloud Computing,Data Security, Cryptology Algorithm.

1. INTRODUCTION

Cloud Computing is Internet Based Computing Whereby Shared Resources, Software, and Information are Provided to Computers and Other Devices on Demand.

There are four areas of pressure that are driving software development to the cloud:
1. Time, cost, and innovation –The project teams need to do more, faster within less budget, cost.
2. Distributed complex sourcing—teams are geographically dispersed.
3. Faster delivery of innovation—focus is on enabling developers to think outside the box in order to deliver business value.
4. Increasing complexity—in today's world, coding for simple project can span several million lines.

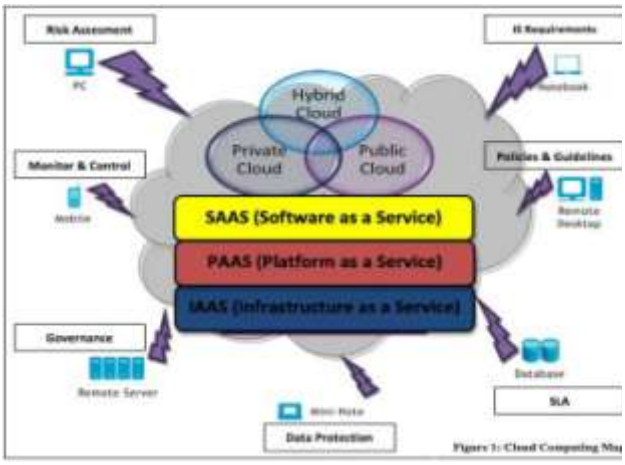
Cloud Computing is emerging approach because of the factors discussed above. In Cloud Computing, service providers provide the storage for data along with services. But due the lack of proper security policies, Cloud Computing adoption is becoming a serious issue.

A cloud computing environment generally requires sending data over the Internet and storing it on a third-party system. The privacy and security risks associated with this model must be weighed against alternatives.

2. TYPES OF CLOUD COMPUTING

PUBLIC: Public cloud services may be free or offered on a pay-per-usage mode. In public Cloud is also known as External Cloud. The services are provided by a third party via Internet, and they are available and are for commercial purposes. Technically there may be little or no difference between public and private cloud architecture, however, security consideration may be substantially different for services (applications, storage, and other resources) that are made available by a service provider for a public audience and when

communication is effected over a non-trusted network. Examples of Public Cloud Computing are Amazon AWS, Microsoft and Google.



PRIVATE: In private Cloud is also known as Internal Cloud. This cloud consists on the hosting of private applications and services for private use (private networks) only.

HYBIRD: Hybrid cloud is a composition of two or more clouds (private, community or public) that remain distinct entities but are bound together, offering the benefits of multiple deployment models. Hybrid cloud can also mean the ability to connect collocation, managed and/or dedicated services with cloud resources.

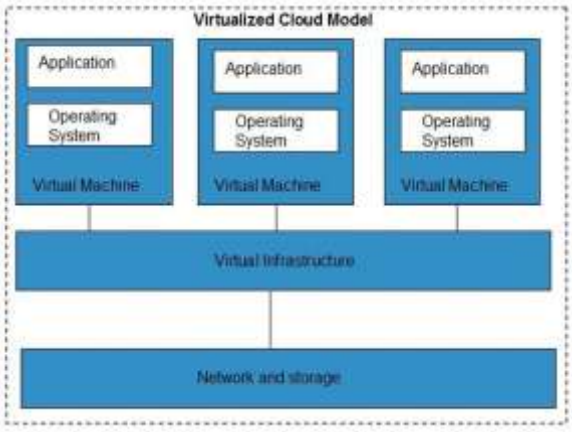
3. CLOUD COMPUTING TECHNOLOGIES

There are certain technologies that are working behind the cloud computing platforms making cloud computing flexible, reliable, and usable. These technologies are listed below:

- Virtualization
- Service-Oriented Architecture (SOA)
- Grid Computing
- Utility Computing

VIRTUALIZATION: Virtualization is a technique which allows sharing single physical instance of an application or resource among multiple organizations or tenants (customers). It does so by assigning a logical name to a physical resource and providing a pointer to that physical resource when demanded.

The Multitenant architecture offers virtual isolation among the multiple tenants and therefore, the organizations can use and customize the application as though, they each has its own instance running.



SERVICE-ORIENTED ARCHITECTURE (SOA): Service-Oriented Architecture helps to use applications as a service for other applications regardless type of vendor, product or technology. Therefore it is possible to exchange of data between applications of different vendors without additional programming or making changes to services.

GRID COMPUTING: Grid Computing refers to distributed computing in which group computers from multiple locations are connected with each other to achieve common objective. These computer resources are heterogeneous and geographically dispersed.Grid Computing breaks complex task into smaller pieces. These smaller pieces are distributed to CPUs that reside within the grid.

UTILITY COMPUTING: Utility computing is based on Pay per Use model. It offers computational resources on demand as a metered service. Cloud computing, grid computing, and managed IT services are based on the concept of utility computing.

4. CLOUD SERVICE MODELS

INFRASTRUCTURE AS A SERVICE (IAAS) – An IaaS cloud offers access to the raw computing resources of a cloud service. Rather than purchasing hardware itself, the cloud customer purchases access to the cloud

provider's hardware according to the capacity required.

PLATFORM AS A SERVICE (PAAS) – A PaaS cloud offers access to a computing platform which allows cloud customers to write applications to run within that platform, or another instance of it. The platform may in turn be hosted on a cloud IaaS.

SOFTWARE AS A SERVICE (SAAS) – A SaaS cloud offers access to a complete software application which the cloud user accesses through a web browser or other software. Accessing the software in this manner eliminates or reduces the need to install software on the client machine and allows the service to support a wider range of devices. The software may in turn be hosted on a cloud platform or infrastructure.

5. SECURITY ISSUES IN CLOUD COMPUTING

Time, cost, innovation are great benefits of cloud computing but still there are significant security concerns of cloud computing that need to be addressed when considering moving critical applications and sensitive data to public and shared cloud environments. Major security issues related to those faced by cloud providers (organizations providing software-, platform-, or infrastructure-as-a-service via the cloud) and security issues faced by their customers are discussed below:

1. Location of Data: Different organizations located in different geographical regions have different requirements and controls placed on access. Because the data is in the cloud, one may not realize that the data must reside in a physical location. The cloud provider should provide the level of security required for different customers and their needs.

2. Access to data: Access control is a key concern, because insider attacks are a huge risk. A potential hacker is someone who has been entrusted with approved access to the cloud. Anyone using the cloud needs to look at who is managing their data and what types of controls are applied to these individuals.

3. Service level agreement (SLA) terms: The SLA serves as a contracted level of guaranteed service between the cloud provider and the customer that specifies what level of services will be provided.

4. Security breach: If a security incident occurs, what support will be provided by the cloud provider?

5. Legal Issues: Providers and customers must consider legal issues, such as Contracts and E-Discovery, and the related laws, which may vary by country.

6. Authentication and authorization: Every organization has its own way to manage authentication and authorization. Every organization must determine if its current authentication system could also work in a secure and reliable way for users in a cloud environment. Apart from that what is the best way to authenticate cloud services but also be insured.

6. CRYPTOGRAPHY

Cryptography can help emergent acceptance of Cloud Computing by more security concerned companies. The first level of security where cryptography can help Cloud computing is secure storage. Cryptography is the art or science of keeping messages secure by converting the data into non readable forms. Now a day's cryptography is considered as a combination of three algorithms. These algorithms are Symmetric-key algorithms, Asymmetric-key algorithms, and Hashing. In Cloud computing, the main problems are related to data security, backups, network traffic, file system, and security of host, and cryptography can resolve these issues to some extents.

SYMMETRIC-KEY ALGORITHMS: The most important type of the encryption is the symmetric key encryption. Symmetric-key algorithms are those algorithms which use the same key for both encryption and decryption. Hence the key is kept secret. Symmetric algorithms have the advantage of not consuming too much of computing power and it works with high speed in encryption.

1. Data Encryption Standard (DES)
2. Advanced Encryption Standard (AES)
3. Triple-DES
4. Blowfish Algorithm

ASYMMETRIC-KEY ALGORITHMS: Asymmetric-key algorithms are those algorithms that use different keys for encryption and decryption. The two keys are: Private Key and Public Key. The Public key is used by the sender for encryption and the private key is used for decryption of data by the receiver. In cloud computing asymmetric-key algorithms are used to generate keys for encryption. The most common asymmetric-key algorithms for cloud are: RSA, IKE, Diffie-Helman Key Exchange.

1. Homomorphic Encryption
2. RSA

3. Diffie-Hellman Key Exchange

Conclusion

Cloud computing is revolutionizing the way business is carried out in various industries (Government, Healthcare, Software etc.), use of information technology resources and services, but the revolution always comes with new problem. One of the major problems associated with Cloud computing is Security. Various Security issues and Algorithms to deal with data security issues are discussed in this paper. This paper also discusses the advantages, Cloud Technologies, services of the cloud and the different deployment models. In future, security algorithms will be implemented producing results to justify the concepts of security for cloud computing and comparing them to find out which is the most efficient one.

REFERENCES

[1] William Stallings, ―Cryptography and Network Security Principles and Practices,‖ Prentice Hall, New Delhi.

[2]http://en.wikipedia.org/wiki/Google_App_Engine

[3] Wayne A. Jansen, ―Cloud Hooks: Security and Privacy Issues in Cloud Computing‖, 44th Hawaii International Conference on System Sciences 2011.

[4] G. Jai Arul Jose1, C. Sajeev2, ―Implementation of Data Security in Cloud, ―in International Journal of P2P Network Trends and Technology- July to Aug Issue 2011.

[5] PriyankaArora, Arun Singh, HimanshuTyagi ―Analysis of performance by using security algorithm on cloud network‖ in international conference on Emerging trends in engineering and management (ICETM2012), 23-24 June, 2012

[6] Farhan Bashir Shaikh, SajjadHaider , ―Security Threats in Cloud Computing,‖ in 6th international conference internet technology and secured transtion,11-14 december,2011,Abu Dhabi, United Arab Emirates

[7] E. Biham and A. Shamir, Differential Cryptanalysis of the Data Encryption Standard, Springer-Verlag, 1993.

[8] B. Schneier, Applied Cryptography, John Wiley & Sons, New York, 1994.

[9]J.L Smith, The Design of Lucifer, A Cryptographic Device for Data Communication, RC 3326, White Plains: IBM Research.

[10]M. Sudha, Dr.Bandaru Rama Krishna Rao, M. Monica ―A Comprehensive Approach to Ensure Secure Data Communication in Cloud Environment, in International Journal of Computer Applications (0975 – 8887) Volume 12– No.8, December 2010.

[11]G. Devi , M. Pramod Kumar "Cloud Computing: A CRM Service Based on a Separate Encryption and Decryption using Blowfish algorithm" International Journal Of Computer Trends And Technology Volume 3 Issue 4, ISSN: 2231-2803,2012, pp. 592-596.

[12] LeenaKhanna, Prof. AnantJaiswal "Cloud Computing: Security Issues And Description Of Encryption Based Algorithms To Overcome Them", International Journal of Advanced Research in Computer Science and Software Engineering 3(3), March - 2013, pp. 279-283.

[13]http://www.tutorialspoint.com/cloud_computing/cloud_computing_quick_guide.htm.