Research Paper Computer Science

A SECURITY ISSUES ON CLOUD COMPUTING

B.Subramani Head Of The Information Technology Department, Dr.N.G.P. Arts And Science College, Coimbatore.

P.N.Indu Vikashini Research Scholar, Department Of Computer Science, Dr.N.G.P. Arts And Science College, Coimbatore.

ABSTRACT

Cloud computing security or, cloud security is an evolving sub-domain of computer security, network security, and, more broadly, for information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications. Cloud Computing is a platform for providing business or consumer IT services over the Internet. The importance of Cloud Computing is increasing and it is receiving a growing attention in the scientific and industrial communities. Cloud computing transforms the way information technology (IT) and it is consumed by promising improved cost efficiencies, accelerated innovation, faster time-to-market, and the ability to scale applications on demand. We describe various service and deployment models of cloud computing and identify major challenges. Let us discuss about three critical challenges: regulatory, security and privacy issues in cloud computing. Some solutions to mitigate these challenges are also proposed along with a brief presentation on the future trends in cloud computing deployment.

KEYWORDS Cloud Computing security, cloud security, Information Technology, Scientific and Industrial Communities, Regulatory, Security and Privacy Issues.

INTRODUCTION:

Cloud computing is receiving a great deal of attention, in both publications among users, from individuals at home. Cloud computing is a subscription-based service where you can obtain networked storage space and computer resources. Cloud computing is to consider your experience with email. Your email client, if it is Gmail, Hotmail, and so on, takes care of housing all of the hardware and software necessary to support your personal email account. When you want to access your email you open your web browser, go to the email client, and log in. The most important part of this is having internet access. Your email is not housed on your physical computer, you access it through an internet connection, and you can access it anywhere. If you are on a trip, at work, or down the street getting coffee, you can check your email as long as you have access to the internet.

Fig 1: Cloud Computing Services

SECURITY ISSUES IN CLOUD COMPUTING:

Security has been always the main source for IT industries when it comes to cloud adoption. In two surveys carried out by IDC in 2008 and 2009 respectively, security came top on the list. However, the cloud computing is an agglomeration of technologies, operating systems, storage, networking, virtualization, each fraud with inherent security issues. For example, network based attacks, denial of service attacks and network intrusion become carry over risks into cloud computing. There are potentials for a new wave of large-scale attacks by the virtualization cloud infrastructure platform.

Availability - The borders on data is available whenever it is required. This is the prime concerns of mission and safety critical organizations. Availability is also extend to the need of migrate to another provider, uptime periods of current provider or long-term viability of the cloud provider.

Data Security – Data security risk stems primarily from loss of physical, personnel and logical control of data. These include virtualization vulnerabilities, *SaaS* vulnerabilities (e.g. a case in which Google Docs exposed private user files), phishing scams and other potential data breaches. Data security risks mentioned in this include data leakage and interception, economic and distributed denial of service and loss of encryption keys. Some risks also arise due to the multi-tenancy and resource-sharing models as pointed out in. The inability to fully segregate data or isolate separate users can lead to undesired exposure of confidential data in the investigation of a situation involving co-tenants. Hypervisor vulnerabilities can also be leveraged to launch attacks across tenant accounts. Data containing social and national insurance details, health data and financial information raise issues about authorization, rights management, authentication and access controls. A data security lifecycle model is shown in Figure 1.1

Figure 1.1: Data Security Lifecycle

3. Third-Party Control: This is probably the prime cause of concern in the cloud. With the growing value of corporate information, third party access can lead to a potential loss of intellectual property and trade secrets. There is also the issue of a malicious insider who abuses access rights to tenant information. The fear of corporate espionage and data warfare also stems from third party control. Provider compliance with regulations such as those on auditing also raise questions on how that can be effected on site in a globally distributed multi-tenant environment [16]. A situation can also arise in which the user becomes locked-in to a particular vendor. This can be due to a difficulty in migrating data to a new vendor. Other risks might arise from the terms of service being obsolete fol-

lowing the merger or acquisition of the cloud provider. A final note on prompt disaster recovery also arises due to third party data control.

4. Privacy and Legal Issues: Data in the cloud is usually globally distributed which raises concerns about jurisdiction, data exposure and privacy. Pearson [33] summarized the main privacy issues of cloud computing. Users are made to give away their personal information without knowing where it is stored or what future purpose it might serve. Organizations stand a risk of not complying with government policies as would be explained further while the cloud vendors who expose sensitive information risk legal liability. Virtual co-tenancy of sensitive and non-sensitive data on the same host also carries its own potential risks. Some legal compliance issues in cloud computing include the Health Insurance Portability and Accountability Act of 1996, which prevents disclosure of individually identifiable health information. Similarly, the Health Information Technology for Economic and Clinical Health Act, regulations requiring notifications of breaches in health data. The Gramm-Leach-Bliley Act, also has similar requirements with regards to financial data. Similarly, the EU Data Protection Directive seeks to secure the privacy and protection of personal data.

LITERATURE REVIEW:

Badger et al proposed that [1] "cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". It represents a paradigm shift in information technology many of us are likely to see in our lifetime. While the customers are excited by the opportunities to reduce the capital costs, and the chance to divest themselves of infrastructure management and focus on core competencies, and above all the agility offered by the on-demand provisioning of computing, there are issues and challenges which need to be addressed before a ubiquitous adoption may happen.

Armbrust et al proposed that [2] These aspects of cloud computing are: (i) The illusion of infinite computing resources available on demand, thereby eliminating the need for cloud computing users to plan far ahead for provisioning. (ii)The elimination of an up-front commitment by cloud users, thereby allowing companies to start small and increase hardware resources only when there is an increase in their needs. (iii) The ability to pay for use of computing resources on a short-term basis as needed and release them when the resources are not needed, thereby rewarding conservation by letting machines and storage go when they are no longer useful. In a nutshell, cloud computing has enabled operations of large-scale data centers which has led to significant decrease in operational costs of those data centers. On the consumer side, there are some obvious benefits provided by cloud computing. A painful reality of running IT services is the fact that in most of the times, peak demand is significantly higher than the average demand. The resultant massive over-provisioning that the companies usually do is extremely capital-intensive and wasteful. Cloud computing has allowed and will allow even more seamless scaling of resources as the demand changes.

Abadi et al proposed that [3] Pointed out that it is hard to maintain ACID (atomicity, consistency, isolation, durability) properties of during data replication over large geographic zones. Data remembrance or persistence remains an issue due to replication and distribution of data even after a user has left a cloud provider.

Kuyoro et al proposed that [4] considered that security plays a very important role in cloud computing. They cited some problems such as security of data storage on a hard disk of another person, the loss of data and the problem of piracy; if hackers use the cloud services, they would offer free or at a cheaper price to full fill their attacks.

Karkouda et al proposed that [5] treated in their work the security of the data warehouses stored in the cloud. They showed that reliance on providers is difficult to build with the traditional architecture of the cloud based on a single provider. This architecture threatens the confidentiality of customer data since they are hosted by a single provider of external risk operate.

Bhadauria et al proposed that [6] in cloud computing environment, the entire data reside over a set of networked resources, enabling the data to be accessed through virtual machines. Since these data centers may lie in any corner of the world beyond the reach and control of users. There are multifarious security and privacy challenges that need to be understood and taken care; they shows several risks that threaten the security of data in the clouds SQL injection attacks, hidden field manipulation and distributed denial of service attacks.

Sajithabanu et al proposed that [7] propose a method to build a trusted computing environment for cloud computing system by providing secure cross platform into cloud computing system. The proposed Network consists of three backup sites for recovery after disaster. The backs up sites are located at remote location from the main server. If any one of the paths fails, it will use alternate path working. The encrypted file will be creating during back up sites and data's are compressed. The data will be decrypted during recovery operation. They proposed a cross-platform integration model by using secure communication via the internet and the utilization of a key for security. To encrypt the dataSHA Hash Algorithm is used for compression, GZIP algorithm is used for symmetric splitting of files and SFSPL algorithm is implemented.

Ruj et al proposed that [8] propose a new model for data storage and access in clouds, their scheme avoids storing multiple encrypted copies of the same data. In this framework, cloud stores encrypted data (without being able to decrypt them) in order to secure data storage. The main novelty of this model is addition of key distribution centers (KDCs). They propose DACC (Distributed Access Control in Clouds) algorithm by employing attribute-based encryption, where one or more KDCs distribute keys to data owners and users. KDC may provide access to particular fields in all records.

Osama Harfoushi et al proposed that [9] this is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

CONCLUSION:

Cloud Computing is a relatively new concept that presents a good number of benefits for its users; however, it also raises some security problems which may slow down its use. Understanding what vulnerabilities exist in Cloud Computing will help organizations to make the shift towards the Cloud. Since Cloud Computing leverages many technologies, it also inherits their security issues. Traditional web applications, data hosting, and virtualization have been looked over, but some of the solutions offered are immature or inexistent. Some surveys have discussed security issues about clouds without making any difference between vulnerabilities and threats. We have focused on this distinction, where we consider important to understand these issues. Enumerating these security issues was not enough; that is why we made a relationship between threats and vulnerabilities, so we can identify what vulnerabilities contribute to the execution of these threats and make the system more robust. Also, some current solutions were listed in order to mitigate these threats. However, new security techniques are needed as well as redesigned traditional solutions that can work with cloud architectures. Traditional security mechanisms may not work well in cloud environments because it is a complex architecture that is composed of a combination of different technologies.

REFERENCES:

[1] Gartner Inc Gartner identifies the Top 10 strategic technologies for 2011. Online. Available: http://www.gartner.com/it/page.jsp?id=1454221. Accessed: 15-Jul-2011

[2] Greg Boss, Padma Malladi, Denis Quan, Linda Legregni, Harold Hall, "Cloud Computing", http://www.ibm.com/developerswork/websphere/zones/hip ods/library.html, October 2007, pp. 4-4

Boneh, D., and Waters, B. (2007). Conjunctive, Subset, and Range Queries on Encrypted Data. In Proceedings of the 4th Conference on Theory of Cryptography *(TCC'07)*, pp. 53-534.

[3] Shankland S (2009) HP's Hurd dings cloud computing, IBM.

[4] National Institute of Standards and Technology -Computer Security Division http://csrc.nist.gov/groups/SNS/cloud-computing/

[5] R. Bhadauria, R. Chaki , N. Chaki, and S. Sanya, "A Survey on Security Issues in Cloud Computing,"*IEEE* Communications Surveys and Tutorials, pp. 1-15, 2011.

[6] N. Antony and A. A. R. Melvin, "A Survey on Encryption Schemes in the Clouds for Access Control," International Journal of Computer Science and Management Research, issn 2278-733x, vol. 1, Issue 5, pp. 1135-1139, December 2012.