www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issue 11 Nov. 2016, Page No. 18823-18826

Cloud computing and security issue

Rajendra kumar
(rajendra888999@gmail.com)

ABSTRACT: *Cloud computing has make the conceptual and structural basis for tomorrow's computing. The World computing structure is rapidly moving towards cloud based architecture. While it is important to take advantages of could based computing by means of moving it in diversified sectors, the security aspects in a cloud based computing environment is most important. Cloud based services and service providers are being evolved which has resulted in a new business trend based on cloud technology. With the introduction of large number of cloud based services and geographically differ cloud service providers, sensitive information of different entities are normally stored in remote servers and locations with the possibilities of being exposed to unauthorized access in situations where the cloud servers storing those information are compromised. If security is not strong and consistent, the flexibility and advantages that cloud computing has to offer will have little credibility. In this paper security in cloud computing is elaborated in a way that covers security issues, concerns and challenges for Data Security in Cloud. This paper presents a review on the cloud computing concepts as well as security issues inherent within the context of cloud computing and cloud structure.*

KEYWORD: Threats to cloud confidentiality, cloud integrity, Cloud Security Alliance, cloud availability & cloud privacy.

INTRODUCTION

Newly research in the field of could computing have immensely changed the way of computing as well as the concept of computing resources. In a cloud based computing structure, the resources are normally in network and accessed remotely by the cloud users As if he wants to take advantage of the cloud, he must ensure the safe network and also utilize the resource allocation and scheduling provided by clouds. The secure data exchange is crucial for any network; so it is very important to take security and privacy into account when designing and using cloud services. Processing is done automatically implying the fact that the data and other elements from a person need to be transmitted to the cloud infrastructure or server for processing; and the output is returned upon completion of required processing. A simple example of cloud computing is Yahoo email, Gmail, or Hotmail etc. You don't need software or a server to use them. All a consumer would need is just an internet connection and you can start sending emails. The server and email management software is all on the cloud (internet) and is totally managed by the cloud service provider Yahoo, Google etc. The consumer gets to use the software alone and enjoy the benefits. The analogy is, 'If you need milk, would you buy a cow ?' All the users or consumers need is to get the benefits of using the software or hardware of the computer like sending emails etc. Just to get this benefit (milk) why should a consumer buy a (cow) software /hardware?

THREATS RELATED TO CLOUD COMPUTING

Cloud Confidentiality

Confidentiality is defined as the assurance that sensitive information is not disclosed to unauthorized persons, processes, or devices. Hence, we must make sure that the users' confidential data, which the users do not want to be accessed by service providers is not disclosed to service providers in the cloud computing systems, including applications, platforms, CPU and physical memories. It is noted that users' confidential data is disclosed to a service provider only if all of the following three conditions are satisfied simultaneously [1]:

Confidentiality is defined as the assurance that sensitive information is not disclosed to unauthorized persons, The current cloud computing system consists of three layers: software layer, platform layer and infrastructure layer. The software layer provides the interfaces for users to use Cloud Service Providers (CSP) CSPs' applications running on a cloud infrastructure. The platform layer provides the operating environment for the software to run using system resources. The infrastructure layer provides the hardware resources for computing, storage and networks [2]. Platforms or infrastructures could be provided as virtual machines. The following are the major problems of current cloud computing system:

Each CSP has a software layer, a platform layer and a infrastructure layer. When users use a cloud application from a CSP, then the users are forced to use the platform and infrastructure provided by the same CSP. Hence the CSP knows where the users' data are located and has full access privilege to the data.

The users are forced to use the interfaces provided by the CSP, and users' data have to be in a fixed format specified by the CSP. Hence, the CSP knows all the information required for understanding the data.

Protecting data from the CSP is more difficult process in the cloud environment. Because, they are privileged admins have rights to monitor users‟ data [3]. They are easily compromised the confidentiality of data stored in the cloud. So, maintaining confidentiality of data is more essential in cloud environment. Ensuring confidentiality helps all types of cloud users to securely store and maintain their data in the cloud.

CROSS-VM ATTACK VIA SIDE CHANNELS:

A Cross-VM attack exploits the nature of multi-tenancy, which enables that VMs belonging to different customers may co-reside on the same physical machine. Aviram et al. [5] regard timing side- channels as an insidious threat to cloud computing security due to the fact that a) the timing channels pervasively exist and are hard to control due to the nature of massive parallelism and shared infrastructure; b) malicious customers are able to steal information from other ones without leaving a trail or raising alarms.

MALICIOUS SYSADMIN:

The Cross-VM attack discusses how others may violate confidentiality cloud customers that co-residing with the victim, although it is not the only threat. Privileged sysadmin of the cloud provider can perform attacks by accessing the memory of a customer's VMs. For instance, Xenaccess [4] enables a sysadmin to directly access the VM memory at run time by running a user level process in Domain.

CLOUD INTEGRITY:

Similar to confidentiality, the notion of integrity in cloud computing concerns both data integrity and computation integrity. Data integrity implies that data should be honestly stored on cloud servers, and any violations (e.g., data is lost, altered, or compromised) are to be detected. Computation integrity implies the notion that programs are executed without being distorted by malware, cloud providers, or other malicious users, and that any incorrect computing will be detected.

Threats to Cloud Integrity:

- **Dishonest computation in remote servers:**

With outsourced computation, it is difficult to judge whether the computation is executed with high integrity. Since the computation details are not transparent enough to cloud customers, cloud servers may behave unfaithfully and return incorrect computing results; they may not follow the semi-honest model. For example, for computations that require large amount of computing resources, there are incentives for the cloud to be"lazy" [5]. On the other hand, even the semi-honest model is followed, problems may arise when a cloud server uses outdated, vulnerable code, has misconfigured policies or service, or has been previously attacked with a root kit, triggered by malicious code or data [6].

- **Data loss/manipulation:**

In cloud storage, applications deliver storage as a service. Servers keep large amounts of data that have the capability of

being accessed on rare occasions. The cloud servers are distrusted in terms of both security and reliability [6], which means that data may be lost or modified maliciously or accidentally. Administration errors may cause data loss (e.g., backup and restore, data migration, and changing memberships in P2P systems [7]). Additionally, adversaries may initiate attacks by taking advantage of data owners' loss of control over their own data.

CLOUD SECURITY ALLIANCE (CSA):

CSA's mission is to promote the use of best practices for providing security assurance within cloud computingand to provide education on the uses of cloud computing to help secure all other forms of computing. Nine CSA working groups are looking into the development of best practices to secure the cloud:

• Group 1: Architecture and Framework
Responsible for technical architecture and related framework definitions.

• Group 2: Governance, Risk, Compliance (GRC), Audit, Physical, Business Continuity Management (BCM), Disaster Recovery (DR) Responsible for governance, risk management, compliance, auditing, traditional/physical security, business continuity management and disaster recovery.

• Group 3: Legal Issues: Contracts and E-Discovery Responsible for legal guidance, contractual issues, global law, eDiscovery and related issues.

• Group 4: Portability, Interoperability and Application Security Responsible for application layer security issues and developing guidance to facilitate portability and interoperability between cloud providers.

• Group 5: Information Management and Data Security Responsible for identity and access management, encryption and key management, identifying enterprise integration issues and solutions.

• Group 6: Data Center Operations and Incident Response Responsible for incident response and forensics, as well as identifying new issues related to cloud based data centre operations.

• Group 7: Information Lifecycle Management and Storage Responsible for data-related issues in the cloud.

• Group 8: Virtualization and Technology Compartmentalization
Responsible for understanding how to compartmentalize technologies used for multi-tenancy,
including, but not limited to, virtualization.

• Group 9: Security as a Service
Responsible for understanding how to deliver security solutions via cloud models.

FRAUDULENT RESOURCE CONSUMPTION (FRC) ATTACK:

A representative Economic Denial of Sustainability attack is FRC [9], [10], which is a subtle attack that may be carried out over a long period (usually lasts for weeks) in order to take effect. In cloud computing, the goal of a FRC attack is to deprive the victim (i.e., regular cloud customers) of their long-term economic availability of hosting web contents that are publicly accessible. In other words, attackers, who act as legal cloud service clients, continuously send requests to website hosting in cloud servers to consume bandwidth, which bills to the cloud customer owning the website; seems to the web server, those traffic does not reach the level of service denial, and it is difficult to distinguish FRC traffic from other legitimate traffic. A FRC attack succeeds when it causes financial burden on the victim.

CLOUD PRIVACY:

Privacy is yet another critical concern with regards to cloud computing due to the fact that customers' data and business logic reside among distrusted cloud servers, which are owned and maintained by the cloud provider. Therefore, there are potential risks that the confidential data (e.g., financial data, health record) or personal information (e.g., personal profile) is disclosed to public or business competitors. Privacy has been an issue of the highest priority [10]. Throughout this text, we regard privacy- preservability as the core attribute of privacy. A few security attributes directly or indirectly influence privacy preservability, including confidentiality, integrity, accountability, etc. Evidently, in order to keep private data from being disclosed, confidentiality becomes indispensable, and integrity ensures that data/computation is not corrupted, which somehow preserves privacy. Accountability, on the contrary, may undermine privacy due to the fact that the methods of achieving the two attributes usually conflict. Threats to Cloud Privacy: In some sense, privacy-preservability is a stricter form of confidentiality, due to the notion that they both prevent information leakage. Therefore, if cloud confidentiality is ever violated, privacy-preservability will also be violated. Similar to other security services, the meaning of cloud privacy is twofold: data privacy and computation privacy.

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 discussed security issues for cloud. These issues include cloud integrity, cloud confidentiality, cloud availability, cloud privacy. There are several threats to cloud confidentiality including cross-VM attack and Malicious sysadmin. On the other hand integrity of cloud is compromised due to data

loss and dishonest computation in remote servers. DoS (Denial of Service attack is the most common attack which is also possible in cloud computing network. This attack attempts to prevent the data available to its intended users. The last issue is cloud privacy and it is similar to cloud confidentiality. if cloud confidentiality is at risk, cloud privacy will

REFRENCES:

[1] DoD Trusted Computer System Evaluation Criteria, http://csrc.nist.gov/publications/history/dod85.pdf.

[2] Stephen S. Yau and Ho G. An "Confidentiality Protection in Cloud Computing Systems", Int J Software Informatics, Vol.4, No.4, December 2010, pp. 35-1365.

[3]Zhang Q, Lu Cheng, and Raouf Boutaba, "Cloud Computing: State-of-the-Art and Research Challenges", Springer Journal of Internet Service Application, Volume 1, Issue 1, 2010, pp. 7-18.

[4]Armbrust M, Fox A, Griffith R, Joseph A. D, Katz R. H, Konwinski A, Lee G, Patterson D. A, Rabkin A, Stoica I, and Zaharia M., "Above the clouds: A Berkeley View of Cloud Computing", EECS Department, University of California, Berkeley, Technical Report, 2009, pp. 1-23.

[5] A. Aviram, S. Hu, B. Ford, and R. Gummadi, "Determinating timing channels in compute clouds," In Proc. 2010 ACM workshop on Cloud computing security workshop (CCSW '10). ACM, New York, NY, USA, 103-108.

[6]B. D. Payne, M. Carbone, and W. Lee, "Secure and Flexible Monitoring of Virtual Machines," In Proc. ACSAC'07, 2007.

[7]Armbrust M, Fox A, Griffith R, Joseph A. D, Katz R. H, Konwinski A, Lee G, Patterson D. A, Rabkin A, Stoica I, and Zaharia M., "Above the clouds: A Berkeley View of Cloud Computing", EECS Department, University of California, Berkeley, Technical Report, 2009, pp. 1-23.

[8] Zhang Q, Lu Cheng, and Raouf Boutaba, "Cloud Computing: State-of-the-Art and Research Challenges", Springer Journal of Internet Service Application, Volume 1, Issue 1, 2010, pp. 7-18.

[9]Sudha M and Monica M, "Enhanced Security Framework to Ensure Data Security in Cloud Computing Using Cryptography", Advances in Computer Science and its Applications, Volume 1, Issue 1, 2012, pp. 32-37.

[10]J. Idziorek and M. Tannian, "Exploiting cloud utility models for profit and ruin," in Cloud Computing (CLOUD),2011 IEEE International Conference on, 2011, pp. 33-40.

[11]Owens, D. (2010). Securing Elasticity in the Cloud. *Communications of the ACM,* Jun 2010, 53(6), 46-51.

[12]Vizard, M. (2010). Assessing the Risks of Cloud Computing, Oct 11, 2010, available at http://www.itbusinessedge.com/cm/blogs/vizard/assessing-the-risks-of-cloudcomputing/?