IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 25-29
www.iosrjournals.org

Cloud Computing and Security Issues in the Cloud

Madhuri Pramanik[1], Vishal Dhabalia[2]
[1](mistimadhuri@gmail.com, G. H. Raisoni Institute of Information Technology, Maharashtra, India)
[2](vishal.dhabalia@gmail.com, G. H. Raisoni College of Commerce Science & Technology, India)

Abstract: *Cloud computing has formed the conceptual and infrastructural basis for tomorrow's computing. The global computing infrastructure is rapidly moving towards cloud based architecture. While it is important to take advantages of could based computing by means of deploying it in diversified sectors, the security aspects in a cloud based computing environment remains at the core of interest. 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 numerous clouds based services and geographically dispersed cloud service providers, sensitive information of different entities are normally stored in remote servers and locations with the possibilities of being exposed to unwanted parties in situations where the cloud servers storing those information are compromised. If security is not robust and consistent, the flexibility and advantages that cloud computing has to offer will have little credibility. 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.*

Keywords: *SaaS, PaaS, IaaS, DDoS, SCC*

I. INTRODUCTION

Recent developments 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 infrastructure, the resources are normally in someone else's premise or network and accessed remotely by the cloud users. Processing is done remotely 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. In some cases, it might be required or at least possible for a person to store data on remote cloud servers. These gives the following three sensitive states or scenarios that are of particular concern within the operational context of cloud computing:

- The transmission of personal sensitive data to the cloud server,
- The transmission of data from the cloud server to clients' computers and
- The storage of clients' personal data in cloud servers which are remote server not owned by the clients.

All the above three states of cloud computing are severely prone to security breach that makes the research and investigation within the security aspects of cloud computing practice an imperative one. There have been a number of different blends that are being used in cloud computing realm, but the core concept remain same – the infrastructure, or roughly speaking, the resources remain

Somewhere else with someone else's ownership and the users 'rent' it for the time they use the infrastructure. In some cases, stored sensitive data at remote cloud servers are also to be counted. Security has been at the core of safe computing practices. When it is possible for any unwanted party to 'sneak' on any private computers by means of different ways of 'hacking'; the provision of widening the scope to access someone's personal data by means of cloud computing eventually raises further security concerns. Cloud computing cannot eliminate this widened scope due to its nature and approach. As a result, security has always been an issue with cloud computing practices. Robustness of security and a secured computing infrastructure is not a one-off effort, it is rather ongoing – this makes it essential to analyze and realize the state-of-the-art of the cloud computing security as a mandatory practice. Cloud is mainly categorized as private cloud, community cloud, public cloud and hybrid cloud Due to its diversified potentiality, the approach to cloud computing is being thought to be as the 5th utility to join the league of existing utilities water, electricity, gas and telephony rather than being just another service.

II. CLOUD COMPUTING INFRASTRUCTURE

The term cloud computing is rather a concept which is a generalized meaning evolved from distributed and grid computing. Cloud computing is described as the offspring of distributed and grid computing by some authors. The straightforward meaning of cloud computing refers to the features and scenarios where total computing could be done by using someone else's network where ownership of hardware and soft resources are

of external parties. In general practice, the dispersive nature of the resources that are considered to be the 'cloud' to the users are essentially in the form of distributed computing; though this is not apparent or by its definition of cloud computing, do not essentially have to be apparent to the users.

In recent years, the cloud has evolved in two broad perspectives – to rent the infrastructure in cloud, or to rent any specific service in the cloud. Where the former one deals with the hardware and software usage on the cloud, the later one is confined only with the 'soft' products or services from the cloud service and infrastructure providers. The computing world has been introduced with a number of terminologies like SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service) with the evolution of cloud computing. As discussed earlier, the term 'cloud computing' is rather a concept, so are the terminologies to define different blends of cloud computing. At its core essence, cloud computing is nothing but a specialized form of grid.

And distributed computing which varies in terms of infrastructure, services, deployment and geographic dispersion. In a pervasive meaning within the context of computer networks, infrastructure could be thought of as the hardware as well as their alignment where platform is the operating system which acts as the platform for the software. This is merely the level of abstraction that defines the extent to which an end-user could 'borrow' the resources ranging from infrastructure to software – the core concern of security and the fashion of computing are not affected by this level of abstraction. As a result, security is to be considered within any form of cloud computing regardless of flavor, hierarchy and level of abstraction. Virtualization is an inevitable technology that is highly coupled with the concept of cloud computing, it is the virtualization technology that complements cloud services especially in the form of PaaS and SaaS where one physical infrastructure contains services or platforms to deliver a number of cloud users simultaneously. This leads to the addition of total security aspects of virtualization technology on top of the existing security concerns and issues of cloud computing.

Figure 1 illustrates a typical cloud based scenario that includes the cloud service provider and the cloud users in a cloud computing architecture.

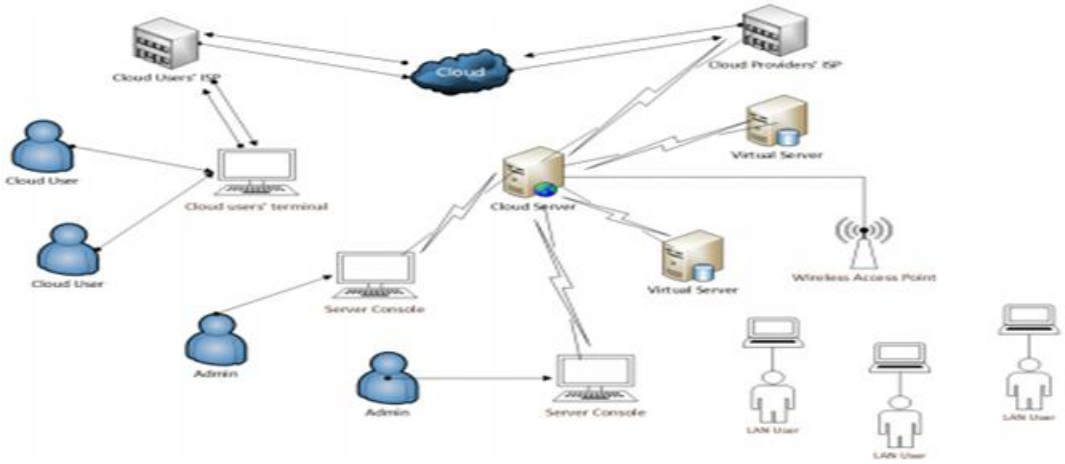

Figure 1: A Typical Cloud Architecture

The illustration of cloud architecture in figure 1 is a simplest one where few complex characteristics of cloud computing (e.g. redundancy, server replication, and geographic dispersion of the cloud providers' network) are not shown – the purpose of the illustration is to establish the arrangement that makes the concept of cloud computing a tangible one. The network architecture is self explanatory with the identification of cloud users when considered in-line with the discussion of the cloud computing concept presented earlier. One notable part from the architecture is that, while the cloud users are clearly identified and named accordingly due to their remote location and means of remote access to the cloud servers, the admin users who are administering the cloud servers are not cloud users in any form with respect to the cloud service provider's network in the scenario. It is arguable whether the LAN users in figure 1 are cloud users or not. Such room for argument could exist due to the phrase 'cloud computing' being a concept rather than a technical terminology. If the definition of cloud computing is taken to have essential arrangements of being the servers located remotely that are accessed through public infrastructure (or through cloud), then the LAN users in figure 1 may not be considered as the cloud users in the context. With respect to distributed and grid computing as the mother technology that define the infrastructural approach to achieve cloud computing, the LAN users in the scenario are essentially the cloud users when they use the cloud services offered by the servers; the LAN users in this perspective are essentially using resources that are 'borrowed' from the servers on an on-demand basis.

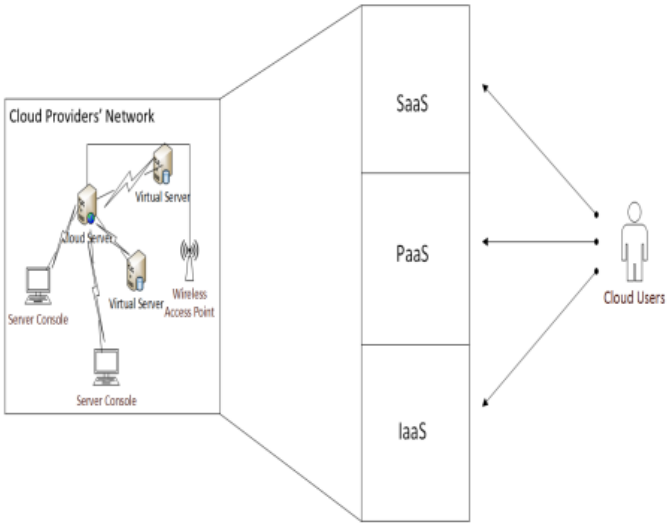

Figure 2: Cloud Service Hierarchy

As depicted in figure 2, the technical details, arrangements and management of the cloud service providers' network is transparent to the cloud user. From the end of the cloud user, the service from the provider comes in the form of SaaS, PaaS or IaaS where the cloud user has no intention or worry about what goes on in the internal arrangement of the cloud service providers' network. Any disruption of any form for whatever is the reason, deem to the cloud users either as service unavailability or quality deterioration – its affect and ways to counter this disruption is a critical part for the cloud infrastructure. Security issues might play a stimulating role as a driving factor for any aforementioned disruption.

III. SECURITY ISSUES IN CLOUD

Cloud computing comes with numerous possibilities and challenges simultaneously. Of the challenges, security is considered to be a critical barrier for cloud computing in its path to success. The security challenges for cloud computing approach are somewhat dynamic and vast. Data location is a crucial factor in cloud computing security. Location transparency is one of the prominent flexibilities for cloud computing, which is a security threat at the same time – without knowing the specific location of data storage, the provision of data protection act for some region might be severely affected and violated. Cloud users' personal data security is thus a crucial concern in a cloud computing environment.

In terms of customers' personal or business data security, the strategic policies of the cloud providers are of highest significance as the technical security solely is not adequate to address the problem. Trust is another problem which raises security concerns to use cloud service for the reason that it is directly related to the credibility and authenticity of the cloud service providers. Trust establishment might become the key to establish a successful cloud computing environment.

The provision of trust model is essential in cloud computing as this is a common interest area for all stakeholders for any given cloud computing scenario. Trust in cloud might be dependent on a number of factors among which some are automation management, human factors, processes and policies. Trust in cloud is not a technical security issue, but it is the most influential soft factor that is driven by security issues inherent in cloud computing to a great extent. All kinds of attacks that are applicable to a computer network and the data in transit equally applies to cloud based services – some threats in this category are man-in-the-middle attack, phishing, eavesdropping, sniffing and other similar attacks. DDoS (Distributed Denial of Service) attack is one common yet major attack for cloud computing infrastructure. The well known DDoS attack can be a potential problem for cloud computing, though not with any exception of having no option to mitigate this. The security of virtual machine will define the integrity and level of security of a cloud environment to greater extent. Accounting & authentication as well as using encryption falls within the practice of safe computing - they can be well considered as part of security concerns for cloud computing.

However, it is important to distinguish between risk and security concerns in this regard. For example, vendor lock-in might be considered as one of the possible risks in cloud based services which do not essentially have to be related to security aspects. On the contrary, using specific type of operating system (e.g. opensource vs. proprietary) might pose security threat and concerns which, of course, is a security risk. Other examples of business risks of cloud computing could be licensing issues, service unavailability, provider's business discontinuity that do not fall within the security concerns from a technical viewpoint. Thus, in cloud computing

context, a security concern is always some type of risk but any risk cannot be blindly judged to be a security concern.

Allocation of responsibilities among the parties involved in a cloud computing infrastructure might result in experiencing inconsistency which might eventually lead to a situation with security vulnerabilities. Like any other network scenario, the provision of insider-attack remains as a valid threat for cloud computing. Any security tools or other kinds of software used in a cloud environment might have security loopholes which in turn would pose security risks to the cloud infrastructure itself. The problem with third party APIs as well as spammers are threats to the cloud environment.

As cloud computing normally means using public networks and subsequently putting the transmitting data exposed to the world, cyber attacks in any form are anticipated for cloud computing. The existing contemporary cloud based services have been found to suffer from vulnerability issues with the existence of possible security loopholes that could be exploited by an attacker. Security and privacy both are concerns in cloud computing due to the nature of such computing approach.

The approach by which cloud computing is done has made it prone to both information security and network security issues. Third party relationship might emerge as a risk for cloud environment along with other security threats inherent in infrastructural and virtual machine aspects. Factors like software bugs, social engineering, human errors make the security for cloud a dynamically challenging one. Intrusion detection is the most important role in seamless network monitoring to reduce security risks. If the contemporary IDSs (Intrusion detection Systems) are inefficient, the resultant consequence might be undetected security breach for cloud environment.

The facets from which the security threat might be introduced into a cloud environment are numerous ranging from database, virtual servers, and network to operating systems, load balancing, memory management and concurrency control. Data segregation and session hijacking are two potential and unavoidable security threats for cloud users. One of the challenges for cloud computing is in its level of abstraction as well as dynamism in scalability which results in poorly defined security or infrastructural boundary. Privacy and its underlying concept might significantly vary in different regions and thus it may lead to security breach for cloud services in specific contexts and scenarios. Data loss and various botnets can come into action to breach security of cloud servers. Besides, multi-tenancy model is also an aspect that needs to be given attention when it comes to security. Security in the data-centres of cloud providers are also within the interests of security issues, as a single physical server would hold many clients' data making it a common shared platform in terms of physical server or operating system. The storage security at the cloud service providers data centres are also directly linked with the security of the cloud services. All the traditional security risks are thus applicable with added degree of potency in a cloud infrastructure which makes the ongoing success of cloud computing a quite challenging one. Confidentiality, availability and integrity are the generalized categories into which the security concerns of a cloud environment falls. Threats for a cloud infrastructure are applicable both to data and infrastructure.

The wide transition to mobile computing practices in recent years has made it imperative to include mobile computing and its associated technologies as an essential part of cloud computing. Resource scarcity as well as other constraints of mobile computing is barriers to cloud computing. The demand of huge data processing is a problem for mobile end-user devices which has been further complemented by the security concerns of mobile cloud computing.

For mobile cloud computing, the device level limitations has inspired researchers to suggest the inclusion of another level of cloud termed as ‘mobile cloud’ to aid the processing of the specific computing and processing for mobile computing devices. The earlier explained broadcast nature of satellite communication and related security issues are equally applicable to the mobile cloud computing due to its being wireless communication. Besides, the addition of mobile cloud into the perspective would add another cloud with all its security issues for a service provider having both mobile cloud and conventional cloud. The addition of mobile cloud in the scenario would boost performance, but it would also add another layer of security issue not only to the mobile cloud users, but also to the total infrastructure of the cloud service provider.

The hierarchical arrangement of cloud computing facilitates different level of extensibility for the cloud users with varying degree of associated security issues. Security issues for cloud computing are described by some authors as an obvious one due to its nature. In a business model, the risks for the consumers are related to and dependent on the relevant approaches and policies of the cloud service providers the consumers are dealing with. Using cloud products or services may lead to security concerns for the consumers if they are not well aware with the type and particulars of the products or services they are to procure or to use in a cloud environment; this is also related to the cloud providers’ identity and reliability. One of the inherent problems in this context is that, the consumers might normally not be able to identify or foresee all the risks involved in the specific cloud transaction they are dealing with or involved in.

IV CONCLUSIONS

Cloud computing has enormous prospects, but the security threats embedded in cloud computing approach are directly proportional to its offered advantages. Cloud computing is a great opportunity and lucrative option both to the businesses and the attackers – either parties can have their own advantages from cloud computing. The vast possibilities of cloud computing cannot be ignored solely for the security issues reason – the ongoing investigation and research for robust, consistent and integrated security models for cloud computing could be the only path of motivation. The security issues could severely affect could infrastructures. Security itself is conceptualized in cloud computing infrastructure as a distinct layer. Security for cloud computing environment is a non-compromising requirement. Cloud computing is inevitable to become the ideal (and possibly the ultimate) approach to business computing though the security barriers along with other issues need to be resolved for cloud computing to make it more viable. Yet, given its total advantages and dynamism and provided it is deployed within an integrated and secured infrastructural framework, cloud computing can offer virtual ownership and access to 'super computers' without procuring them physically. Perhaps this is what inspired coining the term SCC (Scientific Cloud Computing). Research effort has been contributed to develop faster yet secured SCC tools which will greatly influence the pace of research and motivation in various fields together with clouding computing itself. The social implications of cloud computing approaches might emerge with severe impact if robust security models for cloud computing do not exist.

The security issues for cloud computing are not related to the technical and direct security breach only; a number of social inconsistency might also be resulted even without any 'hard' security breach having taken place. The distributed and dispersive processing, transmission and storage features are behind reason. One such example is the obtaining of digital evidences. The evolution of cloud computing might significantly affect the collection and retention of digital evidence. The vastness and potentiality of cloud computing cannot be overlooked, subsequently robust security models for cloud computing scenarios is the most prioritized factor for a successful cloud based infrastructure development and deployment. With the goal of secured exploitation of a Service Oriented Architecture, the security aspects and issues of cloud computing are inherent not only with the elements that from the cloud infrastructure but also with all associated services as well as the ways computing is done both at the users' and the cloud service providers' ends.

The security issues in cloud computing are somewhat sensitive and crucial on the basis of sociological and technological viewpoints – the technological inconsistency that results in security breach in cloud computing might lead to significant sociological impacts. As a result, when dealing with cloud computing and its security issues, technical as well as epistemological factors are equally important to take into consideration. Based on the fact that the impact of cloud computing can include both the technical and social settings, the research on cloud computing and its related concerns are not related only with computing aspects.

Service oriented architecture and other characteristics of cloud computing suggests that the concept of cloud computing would require to analyze the practicality in line with social, business, technical and legal perspectives – all these facets will incorporate security issues either in technical or strategic form. Regardless of the nature of security issues, it can be undoubtedly concluded that the severe adverse effects as a consequence of security breaches in cloud computing, the deployment of any form of cloud computing should deal with the security concerns corresponding to those of the safety critical systems.

REFERENCES

[1]. Millard, Christopher (2013). Cloud Computing Law. Oxford University Press. ISBN 978-0-19-967168-7.

[2]. Singh, Jatinder; Powles, Julia; Pasquier, Thomas; Bacon, Jean (July 2015). "Data Flow Management and Compliance in Cloud Computing". IEEE Cloud Computing **2** (4): 24–32. doi:10.1109/MCC.2015.69.

[3]. Armbrust, Michael; Stoica, Ion; Zaharia, Matei; Fox, Armando; Griffith, Rean; Joseph, Anthony D.; Katz, Randy; Konwinski, Andy; Lee, Gunho; Patterson, David; Rabkin, Ariel Hu, Tung-Hui (2015). A Prehistory of the Cloud. MIT Press. ISBN 978-0-262-02951-3.

[4]. Rochwerger, B.; Breitgand, D.; Levy, E.; Galis, A.; Nagin, K.; Llorente, I. M.; Montero, R.; Wolfsthal, Y.; Elmroth, E.; Caceres, J.; Ben-Yehuda, M.; Emmerich, W.; Galan, F. "The Reservoir model and architecture for open federated cloud computing". IBM Journal of Research and Development

[5]. Kyriazis, D; A Menychtas; G Kousiouris; K Oberle; T Voith; M Boniface; E Oliveros; T Cucinotta; S Berger (November 2010). "A Real-time Service Oriented Infrastructure". International Conference on Real-Time and Embedded Systems.

[6]. Gogouvitis, Spyridon; Konstanteli, Kleopatra; Waldschmidt, Stefan; Kousiouris, George; Katsaros, Gregory; Menychtas, Andreas; Kyriazis, Dimosthenis; Varvarigou, Theodora (2012). "Workflow management for soft real-time interactive applications in virtualized environments". Future Generation Computer Systems**28** (1)

[7]. Attardi, Jim. "Cloud Technology and Its Implication for Quality Service". Retrieved 27 July 2015.

[8]. Armbrust, Michael; Stoica, Ion; Zaharia, Matei; Fox, Armando; Griffith, Rean; Joseph, Anthony D.; Katz, Randy; Konwinski, Andy; Lee, Gunho; Patterson, David; Rabkin, Ariel.