Cloud Computing: A Study on Security Issue and Challenge

Sahaj Ohri[1] Kirti Sharma[2] Gaurav Bagaria[3] Nilam Choudhary[4]
[1, 2] Student [3]Assistant Professor [4]Research Scholar
[1, 2, 3, 4]Department of Computer Science & Engineering
[1, 2, 3, 4]SGUV, Jaipur, Rajasthan, India

Abstract---Cloud computing transforms the way information technology (IT) is consumed and managed, promising improved cost efficiencies, accelerated innovation, faster time-to-market, and the ability to scale applications on demand However, cloud Computing presents an added level of risk because essential services are often outsourced to a third party, which makes it harder to maintain data security and privacy, support data and service availability, and demonstrate compliance. Cloud Computing leverages many technologies With the growing adoption of cloud computing as a viable business proposition to reduce both infrastructure and operational costs, an essential requirement is to provide guidance on how to manage information security risks in the cloud. Security is one of the major issues which hamper the growth of cloud. The idea of handing over important data to another company is worrisome; such that the consumers need to be vigilant in understanding the risks of data breaches in this new environment. This paper introduces a detailed analysis of the cloud computing security issues and challenges

Keywords: Computing, leverages, worrisome, vigilant

I. INTRODUCTION

As organisations seek new ways of driving businesses forward, increasing demands are now placed on computer networks to provide competitive edge and create new opportunities at reduced cost. This has accelerated business and technological initiatives that promise to provide services at comparably low infrastructure and operating costs. The rapid growth of cloud computing is a good example. 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) Cloud computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services. There are four basic cloud delivery models, as outlined by NIST (Badger et al., 2011), based on who provides the cloud services. The agencies may employ one model or a combination of different models for efficient and optimized delivery of applications and business services. These four delivery models are: (i) *Private cloud* in which cloud services are provided solely for an organization and are managed by the organization or a third

Party. These services may exist off-site. (ii) *Public cloud* in which cloud services are available to the public and owned by an organization selling the cloud services, for example, Amazon cloud service. (iii) *Community cloud* in which cloud services are shared by several organizations for supporting a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). These services may be managed by the organizations or a third party and may exist offsite. A special case of community cloud is the Government or G-Cloud. This type of cloud computing is provided by one or more agencies (service provider role), for use by all, or most, government agencies (user role). (iv) *Hybrid cloud* which is a composition of different cloud computing infrastructure (public, private or community). Cloud Computing appears as a computational paradigm as well as a distribution architecture and its main objective is to provide secure, quick, convenient data storage and net computing service, with all computing resources visualized as services and delivered over the Internet [1,2]. The cloud enhances collaboration, agility, scalability, availability, ability to adapt to fluctuations according to demand, accelerate development work, and provides potential for cost reduction through optimized and efficient computing [3-4]. In spite of the several advantages that cloud computing brings along with it, there are several concerns and issues which need to be solved before ubiquitous adoption of this computing paradigm happens. First, in cloud computing, the user may not have the kind of control over his/her data or the performance of his/her applications that he/she may need, or the ability to audit or change the processes and policies under which he/she must work. Second, the cloud customers may risk losing data by having them locked into proprietary formats and may lose control over their data since the tools for monitoring who is using them or who can view them are not always provided to the customers. Data loss is, therefore, a potentially real risk in some specific deployments

II. ARCHITECTURE OF CLOUD COMPUTING

When talking about a cloud computing system, it's helpful to divide it into two sections: the **front end** and the **back end**. They connect to each other through a network, usually the Internet. The front end is the side the computer user, or client, sees. The back end is the "cloud" section of the system.

The front end includes the client's computer (or computer network) and the application required to access the cloud computing system. Not all cloud computing systems have the same user interface. Services like Web-based e-mail programs leverage existing Web browsers like Internet Explorer or Firefox. Other systems have unique applications that provide network access to clients. On the back end of the system are the various computers, servers and data storage systems that create the "cloud" of computing services. In theory, a cloud computing system could include practically any computer program you can imagine, from data processing to video games. Usually, each application will have its own dedicated server. A central server administers the system, monitoring traffic and client demands to ensure everything runs smoothly. It follows a set of rules called **protocols** and uses a special kind of software

called **middleware**. Middleware allows networked computers to communicate with each other. Most of the time, servers don't run at full capacity. That means there's unused processing power going to waste. It's possible to fool a physical server into thinking it's actually multiple servers, each running with its own independent operating system. The technique is called server virtualization. By maximizing the output of individual servers, server virtualization reduces the need for more physical machines. If a cloud computing company has a lot of clients, there's likely to be a high demand for a lot of storage space. Some companies require hundreds of digital storage devices. Cloud computing systems need at least twice the number of storage devices it requires to keep all its clients' information stored. That's because these devices, like all computers, occasionally break down. A cloud computing system must make a copy of all its clients' information and store it on other devices. The copies enable the central server to access backup machines to retrieve data that otherwise would be unreachable. Making copies of data as a backup is called **redundancy**.

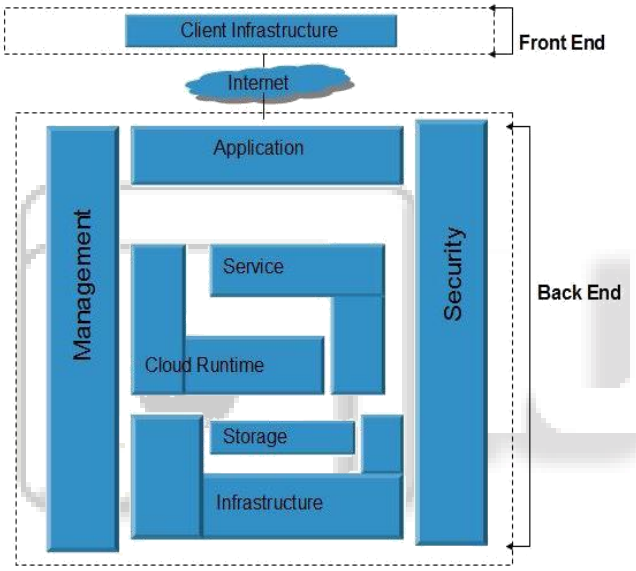

Fig. 1: Architecture of Cloud Computing

III. Security Analysis

Basically Cloud model can be broken down in mainly three layers: **1.** Infrastructure as a service (IaaS) **2.** Platform as a Service (PaaS) and **3.** Software as a Service (SaaS). Here security for each layer has different issues but still they can be closely combined in to one cardinal framework. There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management. Therefore, security issues for many of these systems and technologies are applicable to cloud computing. For example, the network that interconnects the systems in a cloud has to be secure. Furthermore, virtualization paradigm in cloud computing leads to several security concerns

A. Data Security

Data security is a common concern for any technology, but it becomes a major challenge when SaaS users have to rely on their providers for proper security [5,6,7]. In SaaS, organizational data is often processed in plaintext and stored in the cloud. The SaaS provider is the one responsible for the security of the data while is being processed and stored .Also, data backup is a critical aspect in order to facilitate recovery in case of disaster, but it introduces security concerns as well. Also cloud providers can subcontract other services such as backup from third-party service providers, which may raise concerns. Moreover, most compliance standards do not envision compliance with regulations in a world of Cloud Computing . In the world of SaaS, the process of compliance is complex because data is located in the provider's datacenters, which may introduce regulatory compliance issues such as data privacy, segregation, and security, that must be enforced by the provider.

IV. Traditional Security

These concerns involve computer and network intrusions or attacks that will be made possible or at least easier by moving to the cloud. Cloud providers respond to these concerns by arguing that their security measures and processes are more mature and tested than those of the average company. Another argument, made by the Jericho Forum , is: "It could be easier to lock down information if it's administered by a third party rather than in-house, if companies are worried about insider threats… In addition, it may be easier to enforce security via contracts with online services providers than via internal controls." Concerns in this category include:

VM-level attacks. Potential vulnerabilities in the hypervisor or VM technology used by cloud vendors are a potential problem in multi-tenant architectures. Vulnerabilities have appeared in VMWare [9], Xen , and Microsoft's Virtual PC and Virtual Server [8]. Vendors such as Third Brigade mitigate potential VM-level vulnerabilities through monitoring and firewalls.

Cloud provider vulnerabilities. These could be platform-level, such as an SQL-injection or cross-site scripting vulnerability in salesforce.com. For instance, there have been a couple of recent Google Docs vulnerabilities [10] and [12]. The Google response to one of them is here: [11]. There is nothing new in the nature of these vulnerabilities; only their setting is novel. In fact, IBM has repositioned its Rational AppScan tool, which scans for vulnerabilities in web services as a cloud security service (see Blue Cloud Initiative)

Phishing cloud provider. Phishers and other social engineers have a new attack vector, as the Salesforce phishing incident shows.

Expanded network attack surface. The cloud user must protect the infrastructure used to connect and interact with the cloud, a task complicated by the cloud being outside the firewall in many cases. .

Authentication and Authorization. The enterprise authentication and authorization framework does not naturally extend into the cloud. How does a company meld its existing framework to include cloud resources? Furthermore, how does an enterprise merge cloud security data (if even available) with its own security metrics and policies?

Forensics in the cloud. This blog posting on the CLOIDIFIN [12] project summarizes the difficulty of cloud forensic investigations: "Traditional digital forensic

methodologies permit investigators to seize equipment and perform detailed analysis on the media and data recovered. The likelihood therefore, of the data being removed, overwritten, deleted or destroyed by the perpetrator in this case is low. More closely linked to a CC environment would be businesses that own and maintain their own multi-server type infrastructure, though this would be on a far smaller scale in comparison. However, the scale of the cloud and the rate at which data is overwritten is of concern."

V. THREATS IN CLOUD COMPUTING

Threats Cloud computing faces just as much security threats that are currently found in the existing computing platforms, networks, intranets, internets in enterprises. These threats, risk vulnerabilities come in various forms. The Cloud Security Alliance (Cloud Computing Alliance, 2010) did a research on the threats facing cloud computing and it identified the flowing major threats:

- Failures in Provider Security
- Attacks by Other Customers
- Availability and Reliability Issues
- Legal and Regulatory Issues
- Perimeter Security Model Broken
- Integrating Provider and Customer Security Systems
- Abuse and Nefarious Use of Cloud Computing
- Insecure Application Programming Interfaces
- Malicious Insiders
- Shared Technology Vulnerabilities
- Data Loss/Leakage
- Account, Service & Traffic Hijacking
- Unknown Risk Profile

VI. ATTACKS IN CLOUD

Nowadays, there are several attacks in the IT world. Basically, as the cloud can give service to legal users it can also service to users that have malicious purposes. A hacker can use a cloud to host a malicious application for achieve his object which may be a DDoS attacks against cloud itself or arranging another user in the cloud. For example, assume an attacker knew that his victim is using typical cloud provider, now attacker by using same cloud provider can sketch an attack against his victim. Distributed Denial of Service (DDoS) attacks typically focus high quantity of IP packets at specific network entry elements; usually any form of hardware that operates on a Blacklist pattern is quickly overrun and will become in out of- service situation. In cloud computing where infrastructure is shared by large number of clients, DDoS attacks make have the potential of having much greater impact than against single tenanted architectures. If cloud has not plenty resource to provide services to its costumers then this is may be cause undesirable DDoS attacks. Solution for this event is a traditional solution that is increase number of such critical resources. But serious problem is when a malicious user deliberately done a DDoS attacks using bot-net[13]. Most network countermeasures cannot protect against DDoS attacks as they cannot stop the deluge of traffic and typically cannot distinguish good traffic from bad traffic. Intrusion Prevention Systems (IPS) are effective if the attacks are identified and have pre-existing signatures but are ineffectual if there is legitimate content with bad intentions[14]. Unfortunately, similar to IPS solutions, firewalls are vulnerable and ineffective against DDoS attacks because attacker can easily bypass firewalls and also IPSs since they are designed to transmit legitimate traffic and attacks generate so much traffic from so many distinct hosts that a server, or for cloud its Internet connection, cannot handle the traffic [14]. It may be more accurate to say that DDoS protection is part of the Network Virtualization layer rather than Server Virtualization. For example, cloud systems use virtual machines can be overcome by ARP spoofing at the network layer and it is really about how to layer security across multivendor networks, firewalls and load balances.

As more companies move to cloud computing, look for hackers to follow. Some of the potential attack vectors criminals may attempt include:

A. Side Channel attacks

An attacker could attempt to compromise the cloud by placing a malicious virtual machine in close proximity to a target cloud server and then launching a side channel attack

B. Authentication attacks

Authentication is a weak point in hosted and virtual services and is frequently targeted. There are many different ways to authenticate users; for example, based on what a person knows, has, or is. The mechanisms used to secure the authentication process and the methods used are a frequent target of attackers.

C. Man-in-the-middle cryptographic attacks

This attack is carried out when an attacker places himself between two users. Anytime attackers can place themselves in the communication's path, there is the possibility that they can intercept and modify communications.

VII. LEGAL ISSUES

Enterprises are moving their assets to the cloud to capture its many business benefits, including ease of deployment and reducing, if not eliminating, the need for IT infrastructure. However, cloud computing offers an array of pitfalls for the unwary. The unique legal risks and considerations presented by the cloud are especially important and often overlooked by nonlawyers. Here are the top five legal considerations on the way to the cloud.

A. Service levels.

It should go without saying that the starting point should be the business case and intended use of the service, and not any legal document, such as a service level agreement (SLA). Understand what business problem the service will be solving; the intended internal and external users; when, where and how the service will be accessed; whether or not the service is business-critical; the practical consequences if the service is down or degraded for any period of time; and how the use of the service may change over time. Then, ensure the SLA reflects your needs. Almost invariably, SLAs will address availability, planned outages, critical and noncritical outages, service credits and termination rights. Typically, the sole remedy in case of a breach of the SLA is a service credit, which is usually capped based on some percentage of fees paid during the previous 12-month

period. Customers should ask whether the credit is simply window dressing or actually a meaningful economic remedy that would deter the vendor from breaching the SLA.

B. Termination or suspension of service

The software application and/or the data running or housed in the cloud may be critical to your business. Continuity of access and use (to both the application and data), especially when both are on a third-party server, are of utmost importance. To that end, does the cloud vendor in each instance notify you when any of the terms of the agreement may have been violated, and are you given an opportunity to remedy each violation? There is, of course, a delicate balance to be struck here. In a setting where there are multiple customers (tenants), the cloud vendor will have competing obligations to the other customers, and, inasmuch as the actions of one tenant may degrade performance for another, some level of flexibility is required. One approach is to distinguish between the service and the data; in the case of suspension, for example, agree not to lock down access to the data.

C. Representations and warranties; indemnities.

While seemingly arcane, in terms of potential pitfalls, these provisions may be the most important. A representation is a statement of fact, either past or present, while a warranty may express a promise. Typical reps and warranties should confirm that there are no pending or threatened claims of intellectual property right (IPR) infringement and address continued noninfringement, performance (as to the underlying app), and data security and privacy. Breach of a warranty will typically give rise to a limited remedy and thus will be to the exclusion of other remedies, such as money damages. Therefore, be sure the limited remedy makes business sense and will suffice. Note also that cloud providers typically request reps and warranties from the customer, including those pertaining to the customer's data. To that end, the buyer must be careful about the sources of its data or risk exposing itself to liability. An indemnity is a contractual obligation to compensate a party for a loss. Thus, an indemnity would compensate the cloud customer for any claims that its use of the service violated any third-party IP rights, such as patent, copyright or trademark. These suits (especially patent) are costly, so care must be taken to ensure that you are adequately covered.

D. Confidentiality.

Cloud customers should be sure to get satisfactory promises regarding which vendor personnel will have access to confidential information (including customer data) and what steps the vendor will undertake to maintain the confidentiality of that information. Data is king, and this provision deserves considerable attention.

E. Commercial/other.

The considerations above are a good starting point but they are just the tip of the iceberg. Here are a few more to consider: storage fees, if and when there are automatic upgrades; whether or not there are multiple environments (e.g., development, test, and production) available to customer; how customization works in a cloud setting; how many data recoveries does the vendor provide free of charge (and what are the costs of additional backups); and how easy is it to move to another cloud and how will the vendor support the transition?

VIII. Solution of Security Issues

A. Find Key Cloud Provider

First solution is of finding the right cloud provider. Different vendors have different cloud IT security and data management. A cloud vendor should be well established, have experience, standards and regulation. So there is not any chance of cloud vendor closing.

B. Clear Contract

Contract with cloud vendor should be clear. So if cloud vendor closes before contract, enterprise can claim.

C. Recovery Facilities

Cloud vendors should provide very good recovery facilities. So, if data are fragmented or lost due to certain issues, they can be recovered and continuity of data can be managed.

D. Better Enterprise Infrastructure

Enterprise must have infrastructure which facilitates installation and configuration of hardware components such as firewalls, routers, servers, proxy servers and software such as operating system, thin clients, etc. Also should have infrastructure which prevents from cyber-attacks.

E. Use of Data Encryption for security purpose
Developers should develop the application which provides encrypted data for the security. So additional security from enterprise is not required and all security burdens are placed on cloud vendor.

IX. Conclusions

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. However, one must be very careful to understand the security risks and challenges posed in utilizing these technologies. Cloud computing is no exception. In this paper key security considerations and challenges which are currently faced in the Cloud computing are highlighted. Cloud computing has the potential to become a frontrunner in promoting a secure, virtual and economically viable IT solution in the future.

References

[1] Zhao G, Liu J, Tang Y, Sun W, Zhang F, Ye X, Tang N (2009) Cloud Computing: A Statistics Aspect of Users. In: First International Conference on Cloud Computing (CloudCom), Beijing, China. Springer Berlin, Heidelberg, pp 347–358

[2] Zhang S, Zhang S, Chen X, Huo X (2010) Cloud Computing Research and Development Trend. In: Second International Conference on Future Networks (ICFN'10), Sanya, Hainan, China. IEEE Computer Society, Washington, DC, USA, pp 93–97

[3] Cloud Security Alliance (2011) Security guidance for critical areas of focus in Cloud Computing V3.0.. Available: https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf
[4] Khalid A (2010) Cloud Computing: applying issues in Small Business. In: International Conference on Signal Acquisition and Processing (ICSAP'10), pp 278–281
[5] Rittinghouse JW, Ransome JF (2009) Security in the Cloud. In: Cloud Computing. Implementation, Management, and Security, CRC Press
[6] Subashini S, Kavitha V (2011) A survey on Security issues in service delivery models of Cloud Computing. J Netw Comput Appl 34(1):1–11
[7] Viega J (2009) Cloud Computing and the common Man. Computer 42 (8):106–108
[8] VirtualPC vulnerability. http://www.microsoft.com /technet /security/bulletin/ms07-049.mspx.
[9] VMWare vulnerability. http://securitytracker.com /alerts/2008/Feb/1019493.html.
[10] Google Docs Glitch Exposes Private Files. http://www.pcworld.com/article/160927/google_docs_glitch_exposes_private_files.html.
[11] Google's response to Google Docs concerns. http://googledocs.blogspot.com/2009/03/just-to-clarify.html.
[12] Security issues with Google Docs. http://peekay.org/2009/03/26/security-issues-with-google-docs/.
[13] P. Coffee, "Cloud Computing: More Than a Virtual Stack," ed: salesforce.com.
[14] http://cloudsecurity.trendmicro.com/

