An Analysis on Security Concerns in Cloud Computing

Abhishek kumar
M.Tech, Department of Information Technology
Amity School of Engineering and Technology
Amity University, Noida, Uttar Pradesh

Shubham Kumar Gupta
M.Tech, Department of Information Technology
Amity School of Engineering and Technology
Amity University, Noida, Uttar Pradesh

Animesh Kumar Rai
M.Tech, Department of Information Technology
Amity School of Engineering and Technology
Amity University, Noida, Uttar Pradesh

Vikas Deep
Assistant Professor, Department of Information Technology
Amity School of Engineering and Technology
Amity University, Noida, Uttar Pradesh

Abstract -Cloud computing is the emerging technology that is used worldwide for storage as well as distributed data processing. In the cloud technology, client's data is stored on the Cloud service provider's domain. The concept of this new technology i.e. cloud computing is adopted by many clients, but is receiving criticism from many people, who observe that; in this cloud technology, client loses control on computing processes. This paper mainly aims to the fundamental security issues that existing in present cloud computing environments. The fundamental issues that affect the trust between client and service provider are Security, Privacy, Accountability, Auditability and Fault recovery. These issues are the major restriction factor in the development and adoption of cloud computing. In this proposed Trusted Framework for Cloud Computing, we consider the above mentioned trust issues (Security, Privacy, Auditability, Accountability, and Fault Recovery) as the trust component. This framework introduced System Controls Mechanism that are used for establish the trust into system.

Keywords: - Cloud Computing, Distributed, data processing, Trusted Framework, System Controls Mechanism.

I. INTRODUCTION

Internet is the interconnected network of computers all over the world.. People profoundly depend on Internet because they used internet for resource sharing, mailing and information searching etc.. In the beginning of the Internet, very limited services were offered but as soon as time passing, the services of internet is growing and the research is focus to provide everything on Internet as service. Another important part is our desktops having very limited storage capacity, memory power, computing capacity and software etc. If any user wants to store documents, images, videos in his limited storage and let you wants to install heavy software but if computer haslimited resources like storage disk and memory capacity, then system cannot support such type of tasks.

Data mining applications is one of good example because various data mining applications or task process vast data to find out meaningful and useful pattern of information. So it is required more resources to process vast data as fast as possible. In such type of case users are required to increase their storage capacity, computing power and also the size of memory This new technology that is known as Cloud computing is capable to break all these barriers. The NIST (National Institute of Standards and Technology) definition of Cloud computing is as follows:

“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.” [1]

Fundamental characteristics of Cloud Computing are resource-pooling, metered service, on-demand self-service, rapid-elasticity and broad network assess [1]

The NIST definition [1] further classified cloud in three categories according to the deployment of application into the cloud. The cloud service provider’s deployment model specifies that who can gain access to the particular service of cloud. There are three types of clouds:

1.1 Public Cloud

In these model providers offers cloud infrastructure and resources to the general public.The user’s data isadded to the cloud into shared infrastructure. This type of cloud runs by third party and applications and data from different user or client resides together on same cloud server storage and network.

1.2 Private Cloud

Private cloud is known as internal cloud. These types of clouds are intended for specially use by a single client or organization. Private clouds may be managed and built by the external providers or by the organization. The private clouds offer the maximum level of control over consistency, security and performance.

1.3 Hybrid Cloud

In the hybrid cloud environment multiple private and public cloud models are combined together. Hybrid clouds initiate the complexity of determining that how to allocate and distribute various applications across both a private and public cloud.

Cloud Service Model can be further categorized into three service models, these models are also mentioned in the NIST document [1]. These three models are Software as a Service (SaaS), Infrastructure as a Service (IaaS),and Platform as a Service (PaaS). Each service model of cloud virtualizes aspects of storage, computation and networking[1].

II. A SURVEY ON SECURITY ISSUES IN CLOUD COMPUTING

In the cloud computing infrastructure, the whole data of client resides on a set of network resources, which enables the data, which is reside in data centres to be accessed by client through the virtual machines. These data centres can lie in anywhere in the world and the user will not be able to reach and control the data, So that there are a lot of multifarious security concerns and privacy challenges are there that should be well understood and must be taken care of.

According to a survey which is conduct by “The National Institute of Standards and Technology” (NIST) [5] the main challenges which anticipated the adoption of cloud computing environment is security and it rated with a 74.6% , as shown in given figure below, security is higher than all other issues :

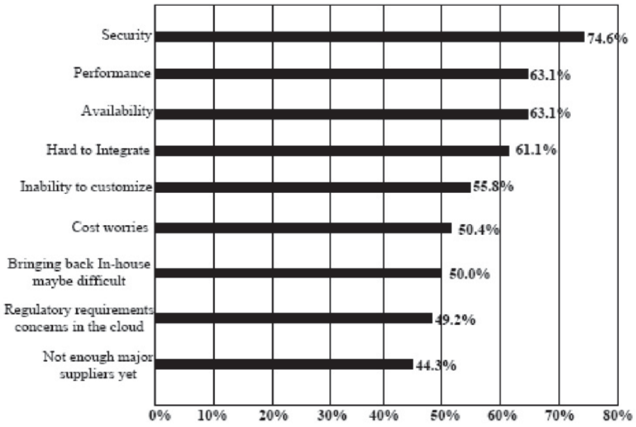


Fig 1: Challenges that expected from adoption to cloud computing (NIST, 2009)

The above figure clearly describes that almost all organizations are worried about the implementation of security mechanism in cloud computing infrastructure.

The following list have some major security issues consider by the Gartner[8] that should be consider as a prerequisite by organizations and all key decision makers whenever deal with Cloud computing vendor [8]:
2.1. Privileged access - This security issue always considers about specialization or privilege for accessing the client's data and "Who will decide about the hiring as well as management of administrator?"
2.2. Regulatory compliance - In this issue organization should consider that "Is the Cloud Service Provider (CSP) eager to go through by an external audits or security certifications?"
2.3 Data location - In this issue client should consider about the control or any decision on location of data because the data centres are operated by the cloud service provider.
2.4 Data segregation - This means, "Is encryption techniques available for data at all stages, andwere those encryption techniques had designed as well as tested by any experienced professionals?"
2.5 Investigative Support - It issues means "Does the service provider have the effective ability for investigation of any illegal or inappropriate activity?"
2.6 Data availability - In this issue the client of CSP should be aware about "Can the cloud provider move all their users data into a different environment should the present environment turns into unavailable and compromised?"

III THREATS TO SECURITY IN CLOUD COMPUTING

The fundamental concern in cloud computing environments is to establish and provide security around isolation and multi-tenancy, giving clients and organizations more relieve besides the "trust us" proposal of clouds . There is a survey report that classifies security issues and threats in cloud computing based on the character of the service delivery infrastructure or environment of the cloud computing system Service delivery model is the basic aspects that should be considered for any comprehensive survey on the cloud computing security model. Security at many different levels like Application level, Network level, as well as Host level is compulsory to keep the cloud efficient up as well as running continuously. Various types of security threats may occur in accordance with different levels.
3.1. Basic Security Attacks - Web 2.0, a basic technology in the direction of enabling the utilization of Software-as-a-Service (SaaS) relieves the client or users of cloud from tasks like installation and maintenance.Web 2.0 has been used worldwide from its beginning. And as the client community that are using Web 2.0 technology is increasing, the security of cloud data has become further important than ever for such an environment.

SQL injection attack is the one of attack in which the malicious code is include into thestandard SQL code and using this the attackers finally gain the unauthorized access to the users database and also he becomes able to retrieve sensitive data and information of user. In some cases the input data of attacker is misunderstood by web-sites they treated it as the user data and allows attacker to access by SQL server and this situation lets the hacker to have know-how of functioning of the web-site and how to make changes into it.

Cross Site Scripting (XSS) attacks, this attack injects malicious scripts or code into Web. The website can be known as dynamic or static based on the types of services provided. Static websites generally don't experience the security threats while the dynamic website does because dynamism property in providing user multi-fold services.

*Man in the Middle attacks (MITM).*MITMis the class of attack that is much popular inthe software-as-a-service (SaaS) environment. In these types of attack, an attacker tries to intrude in ongoing communication between the sender and the client to inject false or fake information and to get knowledge of important data or information communicated between them. There are various types of tools that implementing strong encryption technique such as Dsniff, Wsniff, Cain, Airjack, Ettercap, etc have been implemented and developed for provide safeguard against these threats.

3.2. Network Level Security - Networks can be classified into several types such as shared network, non-shared networks; private or public network, small area network or large area network and every one of them have a verity of security issues and threat. In order to ensure network security given points like integrity and confidentiality in the network, proper access mechanism as well as maintaining the security against any external third-party issue or threats must be considered when providing network-level security.

DNS Attacks - The Domain-Name-Server (DNS) server basically performs the task of translation of any domain name to corresponding IP address. Even though using a DNS security measure such as Domain-Name-System-Security-

Extensions(DNSSEC)always reduces the overall effects of DNS security threats and issues but still there are many cases when these security solutions and measures are proved to be not enough when the connection between a the sender and the receiver is getting rerouted by an evil connection .

Sniffer Attacks - There are such types of application that launch attack by capturing the packets when they flowing in the network and if the information that is transferred by these packets is not using encryption, then it can be read as well as there is a chance that the information that flowing through the network can be captured or traced. A sniffer program, through the (NIC) ensures that data or traffic correlated to other systems which also exist on the network is also gets recorded. This can achieve by placing the Network Interface Card (NIC) in promiscuous mode then in promiscuous mode it will track all information, transmitted on the same network. A malicious-sniffing-detection platform that is based on Address Resolution Protocol (ARP) and Round Trip Time (RTT) , that is basically used to detect a sniffing-system that is running on a network [2].

Issue of reused IP addresses - Every node of the network is has an IP address hence an IP address is definitely a finite quantity. There are a large number of cases that are related to reuse of IP address issue have been observed. When a client or user moves out to the network then IP address that is associated with him earlier is assigned to new users. This sometimes may be risks to security of the new user because there is a always certain time-lag between the change of the previous IP-address in the DNS server and the clearing of that particular address from DNS caches. Hence, we can observe that though the previous IP-address is assigned to the new user but still there is always a chances of accessing the information by other user and it is not negligible because the address still exists in the DNS server cache and the data belonging to that particular user can become accessible to other user and that is violating the privacy of original user.

3.3. Application Level Security -

In the application level security we can use the software as well hardware resources in order to provide the security to the applications in such a way that the attackers should not be able to obtain control on the applications as well as make any desirable changes into their format.In the virtual environment, many companies that work with virtualization technique such as VMware are also using Intel-Virtualization-technology for the security base and the better performance. The threats and security issues that break down application-level-security are:

Security concerns with the hypervisor

Cloud Computing depends basically on the virtualization concepts. In the virtualization technology, the hypervisor is basically defined as the controller and it is known as the virtual machine manager (VMM) and that allows multiple operating-systems to be run on a single system at a time, it provides the resources to every operating-system in such a way that they can’t interfere with each.As the operating systems that are running on the hardware unit increased, the security issue that are concerned with those that of the new operating-systems also needs to be considered. There are multiple OS is running on the single hardware infrastructure, so it is never possible that keep track all the OS and thus maintaining all these operating systems securely is very difficult. It is always possible that a guest or visitor system tries to run a malicious script or code on the provider host system and that can bring the overall system down or can take full control of the system and can block the access to other guest-operating-systems (GOS) [3].If any attacker is being able to get control to hypervisor, he can get control on all the data and information that is passing through that hypervisor.

Denial of service attacks - A denial of service attacks (DoS) is an attempt to make unable the services that is assigned to an authorized user to be used by them. In this type of attack, the server providing the service to the users is extremely flooded by a huge number of requests so that the services become unavailable to any authorized client or user. The occurrence of the denial of service attacks (DoS) increases tremendous bandwidth consumption that causing congestion, and making some parts of the cloud system inaccessible to the authorized users [6].

Cookie poisoning - It this type of attack the change and modification in the contents of cookies is made in order to gain unauthorized access to any particular application or to a webpage by an attacker. The identity related credentials of the user basically contained by these cookies and once these cookies have accessible by attacker; the identity related content of these cookies can be used to impersonate any authorized user. This problem can be avoided by either performing regular cookie-clean-up or by implementing the encryption scheme for the cookies data [2].

Hidden field manipulation - While accessing the web page of any cloud website or application, there are several fields that may be hidden and that contains the web page related information that is basically used by the developers of application or web page. Although, such types of fields in web pages are highly prone to the attacker, hacker can attack because they can be modified easily and then that can be posted on the web-page or underlying application. This may be result in the violation of severe security [3].

Backdoor and debug options - A common practice of the developers of any cloud application or any web site is to enable the option of debug while he publishing an application or the web-site. This option enables the developer to make any developmental changes in the code when needed and then implemented them in the web-sites. Because these options of debugging is facilitate backend entry for the developers, sometimes these option for debug are left enabled unnoticed, and this type of error can provide an simple entry to a attacker into the application or web-site and he can make changes into the web-site or application level [7].

Distributed denial of service attacks - DDoS is the advanced version of Denial of service (DoS) attacks. In the distributed denial of service attacks (DDoS) the attack is spread from many different dynamic networks which is already being compromised unlike DOS.

The DDoS attack is basically run by three fundamental units: first one is a Master, second one is a Slave and finally a Victim. Mater is the attack launcher that play the major role in all these attacks that are causing DDoS, Slave is act like launch pad in the network for the Master. It basically provides the main platform for the Master to launch the DDoS attack on the Victim cloud. Hence it is also known as the co-ordinated attack.

Method that is commonly used against DDoS attach is to contain IDS on all physical machines which holds the user's virtual-machines [35]. This method performs reasonably well in the Eucalyptus cloud.

Security requirement for a secure Cloud computing - International Standards Organization (ISO) defined a standard ISO 7498-2 that states that prevention, detection and elimination all are needed to control and minimize threat in Information Security. Same concept is followed in Cloud computing, but prevention and detection processes are difficult to implement due to complex nature of Cloud. Security requirement for a secure Cloud computing are:

A. Identification and authentication - Users are provided rights to access information in Cloud, but the access can be limited by some constraints. Information Assurance (IA) Technology Professionals defined that Cloud provider controls the access privileges of Cloud user. Users or enterprises are provided a unique ID and corresponding password for their identification and level of services are provided to that authenticated entity after successful verification.

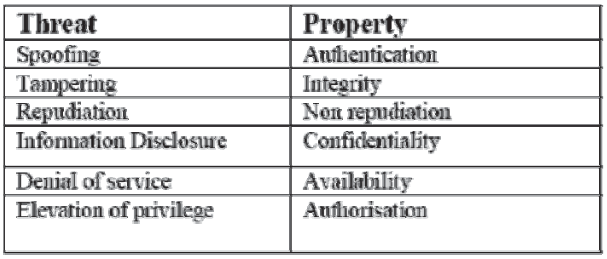
B. Authorization - Authorization ensures that integrity of the Cloud is maintained, thus it plays an important role in security of Cloud. Information Assurance team stated that any organizations will be immune from damage from insiders if authorized access is maintained to protected information assets.

C. Confidentiality - In Clouds, Data or information is stored across multiple distributed databases and any attacker can access data if confidentiality is not kept under notice during development of Cloud. Confidentiality ensures that only authorized data can only be accessed by authorized users not by any unauthorized user. Safety of

D. Integrity - The integrity ensures that Cloud data is not modified or tampered. So Cloud should be in same state if no authorized operation is performed on Cloud. Unauthorized alteration or modification of Cloud data may lead to low trust rating of Cloud.

E. Non-repudiation - Non-repudiation is a major problem in Cloud as it cannot be proved that whether that action was performed or not. Jun Feng showed that applying token provisioning in Cloud applications for data transmission using digital signature and confirmation receipts (i.e. digital receipt of message sent or received confirmation) may ensure non-repudiation.

F. Availability - Availability is major requirement for information security in Clouds .The NIST [1] defined Availability as whether resources of any Cloud are accessible or available to Cloud user or not. It can be affected permanently or temporarily. It can be attacked by blocking some resources so that Cloud user cannot access them anymore, such attacks are equipment outages, Denial of service attacks, and natural disasters etc



Threat	Property
Spoofing	Authentication
Tampering	Integrity
Repudiation	Non repudiation
Information Disclosure	Confidentiality
Denial of service	Availability
Elevation of privilege	Authorisation

Fig 2: Threat to property mapping

Microsoft used STRIDE approach to classify threats, in which threats are classified as Information Disclosure, spoofing, Tampering, Repudiation, DoS and Elevation of privilege. Mapping is performed on the basis that spoofing is faking someone's ID.

Tampering is alteration or modification (unauthorized) of data in Cloud, repudiation is denying a performed action, Information disclosure is access to authorized data by unauthorized user, denial of service is to prevent any genuine user to access Clouds resources and elevation of privileges is getting access without proper authorization.

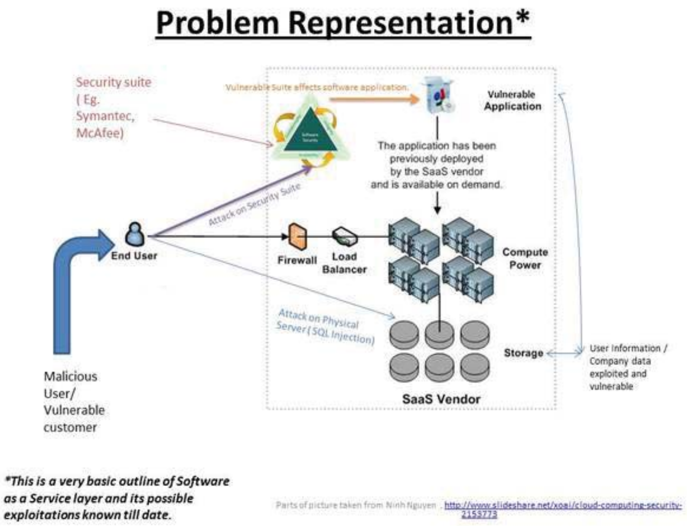
IV. PROBLEM STATEMENT

In cloud computing paradigm, client's data and information is stored at the Cloud Service Provider's data centre. In such type of scenario many issues arises between the client and the cloud service provider. The fundamental issues that affect the trust between client and service provider are Security, Privacy, Accountability, Audit ability and Fault recovery. These issues are the major restriction factor in the development and adoption of cloud computing.

For a trusted cloud computing environment the cloud service provider must ensure the client that the underling cloud infrastructure will provide security, privacy, accountability, auditability and fault recovery. And this can be possible only if the service provider has a trusted cloud infrastructurethat concern and deal with all above mentioned issues.

V. PROPOSED FRAMEWORK FOR BUILDING A TRUSTED CLOUD COMPUTING ARCHITECTURE

As stated in the Problem Statement of this thesis the clients of cloud always expect Security, Privacy, Auditability, Accountability, and Fault Recovery from the Cloud Service Provider (CSP). These are the fundamental trust issues that a client always concern before adopt the cloud computing environment.


Problem Representation*
Security suite (Eg. Symantec, McAfee)
Vulnerable Suite affects software application.
Vulnerable Application
The application has been previously deployed by the SaaS vendor and is available on demand.
Attack on Security Suite
End User
Firewall
Load Balancer
Compute Power
Attack on Physical Server (SQL Injection)
Storage
User Information / Company data exploited and vulnerable
SaaS Vendor
Malicious User/ Vulnerable customer

This is a very basic outline of Software as a Service layer and its possible exploitations known till date.

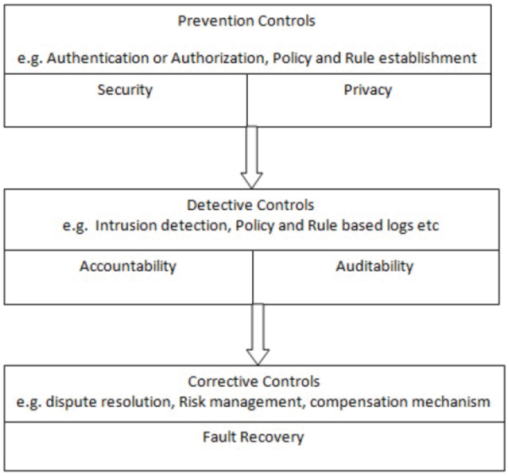
Parts of picture taken from Ninh Nguyen , http://www.slideshare.net/xoai/cloud-computing-security-2153773

In this proposed Trusted Framework for cloud computing we consider the above mentioned trust issues (Security, Privacy, Auditability, Accountability, and Fault Recovery) as the trust component, Hence without concerning about these issues before providing service to the client a cloud computing environment cannot be a trusted. We considering these five issues as primary trust component and providing a solution for these issues by proposing a framework called Trusted Framework for Cloud Computing. This framework introduced System Controls Mechanism that are used for establish the trust into system. These System ControlsComponents handle all above mentioned trust issues in order to achieve trust in cloud computing environment. There is also a trust management system in this framework that is used for evaluation of trusted components with help three type of evaluators. Finally the step by step activities of system execution is described in order to achieve trust is this framework.

A System Architecture

The proposed Trusted Framework for cloud computing consists of following entities:

1. Client of underling cloud computing architecture
2. Primary Trust Components
3. System Controls Component
4. Needed Logs
5. Security Control Module
6. Security Level surveyor
7. Feedback surveyor
8. Reputation Trust surveyor


Prevention Controls
e.g. Authentication or Authorization, Policy and Rule establishment
Security
Privacy
Detective Controls
e.g. Intrusion detection, Policy and Rule based logs etc
Accountability
Auditability
Corrective Controls
e.g. dispute resolution, Risk management, compensation mechanism
Fault Recovery

VI. CONCLUSION AND FUTURE WORK

The proposed Trusted Framework for Cloud Computing considers the five basic trust issues i.e. Security, Privacy, Audit ability, Accountability, and Fault Recovery. In this proposed framework the trust is achieved in the cloud computing environment through the technical as well as policy based approach.This framework gives a novel design approach that can achieve trustworthy service oriented architecture in the cloud environment using enforcement of strong audit ability. This architecture achieves strong audit ability as well accountability using logged information of the end client.

We focused on one design possibility that can improve load balancing in the cloud by carefully distributing the servicerequests among data centers in a clouding computing system.We took a systematic approach and formulated the serviceRegarding to security in cloud computing jointly with thepower flow analysis. In the future a separate Firewall system for cloud system can be implemented using the details of logs which are used in this proposed architecture in order to prevent intrusion based on behavior analysis of client and all other entities that want to access into cloud. Also the implementation with current technologies can be done to implement this framework to achieve trust by existing cloud infrastructure.

REFERENCES

[1] Peter Mell, Timothy Grance, “NIST Definition of Cloud Computing v15,” 2011 www.csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc.

[2] K. Vieira, A. Schulter, C. B. Westphall, and C. M. Westphall, “Intrusion detection techniques for Grid and Cloud Computing Environment,” IT Professional, IEEE Computer Society, vol. 12, issue 4, pp. 38-43, 2010.

[3] D. Gollmann, “Securing Web Applications,” Information Security Technical Report, vol. 13, issue. 1, Elsevier Advanced Technology Publications Oxford, UK, DOI: 10.1016/j.istr.2008.02.002. 2008.

[4] Claudio Mazzariello, Roberto Bifulco and Roberto Canonico, “Integrating a Network IDS into an Open Source Cloud Computing Environment,” Sixth International Conference on Information Assurance

[5] Jain, P.; Rane, D.; Patidar, S.; "A survey and .analysis of cloud model-based security for secure cloud bursting and aggregation in renal environment," Information and Communication Technologies (WICT), World Congress on, vol., no., pp.456-461, 2011

[6] Ghemawat S, Gobioff H, Leung “The Google file system”. Proceeding SOSP '03 Proceedings of the nineteenth ACM symposium on Operating systems principle Pages 29-43, 2003.

[7] Hadoop Distributed File System, www.hadoop.apache.org.

[8] Brodkin, J. (2008, July 02). “Gartner: Seven cloud computing security risks”, see InfoWorld: http://www.infoworld.com/d/security-central/gartner- seven-cloud- computing-security-risks-853.

[9] Hanqian Wu; Yi Ding; Winer, C.; Li Yao; , "Network security for virtual machine in cloud computing," Computer Sciences and Convergence Information Technology (ICCIT), 2010 5th International Conference on , vol., no., pp.18-21, Nov 30 2010.