# A Survey in Top Security Threats in Cloud Computing

Toa Bi Irie Guy-Cedric
Research scholar, Jain University,
Bangalore-560043, India

Dr. Suchithra R
Jain Global Campus, Jain University
Bangalore, India

***Abstract*—Cloud computing is a new technology adopted by many companies and users. Cloud computing presents itself on the market by its main service models, called IaaS, PaaS and SaaS, which offer advantages in capital expenditure through the application, which costs consumers pay for the resources used. But cloud computing has many threats that must be identified and understood to help users and cloud providers make informed decisions about risk mitigation within a cloud strategy.**

***Keywords—Cloud computing, Threats.***

## I. INTRODUCTION

Cloud computing is a new technology in recent years, it aims to facilitate the relocation of data and applications on infrastructure dematerialized accessible from Interne. Many researchers, organizations, governments, business; have tried to define the cloud. According to [1] National Institute of Standards and Technology (NIST), Cloud computing is a model for Enabling ubiquitous, 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 efforts or Service provider interaction. This cloud model is composed of five essential characteristics, three models Service (PaaS, IaaS, and SaaS) and four deployment models (public, private, community, and hybrid), assume as shown in figure1.As with any major technological transition period, the evolution of "cloud computing" is also linked to major security problems, and has generated the greatest interest and questions in the media world. Several organizations and researchers have identified various security-related threats and proposed solutions to address them. In the remainder of our paper we choose to take the major threats for cloud computing according to [2] Cloud Security Alliance (CSA) and in the second part we identify some threats and discuss various solutions proposed.

## II. THREAT IN CLOUD COMPUTING

Security in the cloud is very important given all the variety of vendors and model of deployment; and no different IT security.

In this section the major threats for cloud computing according to Cloud Security Alliance (CSA) are explored and we can divide in three parts data threat, network threat and human threat. The various threats attacks in cloud computing is mentioned as shown figure 1.

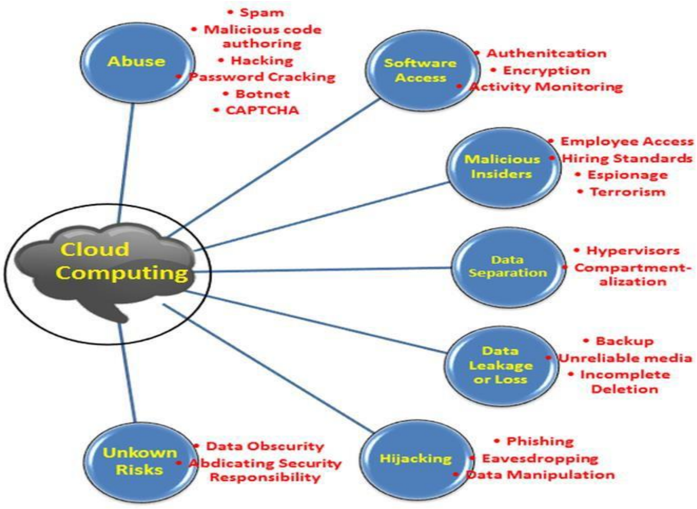

Figure 1: Seven Threats in Cloud computing [1].

### A. *Data Threats*

*Data Breaches*

Data breach is a serious issue in cloud computing. It is defined by the breach of customer data or company by people who do not have permissions. In November 2012, (CSA) researchers from the University of North Carolina, the University of Wisconsin and RSA Corporation released a paper describing how a virtual machine on the a same server could use side channel timing information to extract private cryptographic keys being used in other virtual machines. Sometimes an attacker doesn’t need to go depth but this an important breach of security data, that block user to adopt cloud computing. This is a real issue from a multitenant cloud service database because with a lot of clients, there do not properly designed a security around the data , and the consequences is an attacker can exploit that breach to access of all data from one and all users using the same virtual server. To avoid access of data from other users, applying encryption on data that makes data totally unusable and normal encryption can complicate availability. Before uploading data into the cloud the users are suggested to verify whether the data is stored on backup drives and the keywords in files remain unchanged.

Xiuli Song et al. [3] proposed an efficient encryption and verification scheme for preserving electronic evidence in cloud computing, with various formatting, which can ensure the confidentiality and integrity of the electronic evidence in cloud computing environment.

*Data Loss*

Loss of sensitive data or normal data is a nightmare for consumers, businesses and companies. Indeed loss data is not only the fault of attackers but can be also due of a wrong manipulation of consumers, or also a fire in data center. These are why cloud providers uses technologies backup to preserve data of consumers. To prevent data loss in cloud, different security measures can be adopted. R Chow et al. [4] proposed the usage of Trusted Computing to provide data security. A trusted server has the main functions to control, verify data by cloud server and provide a resume of data activity for the owner of data. The data owner can verify and confirm that he is the only one to have access to its data.

Pasquale puzio and al. [5] proposed a software solution, clouded up that provides both duplication and encryption and retains benefits offered by each technique. Clouded up makes use of convergent encryption but prevents the dictionary attacks (the dictionary attack, in which an attacker manages to generate a potential encryption key and, by comparing the two cipher texts, check whether a file has already been stored or not).

Tomoyoshi T. et al. [6] proposed a system to protect moving data of a company inside a USB even if it is lost; and describe the protection of document in its complete life cycle and avoiding data loss through emails. The encryption, key management, identity management and access fields are applicable on IaaS, PaaS and SaaS models.

### B. Networks Threats

*Denial of Service*

Attacks DoS (Denial of Service) attacks are frequent today and touch three important layer of OSI model (layer 3, 4 and 7) in network and cloud network, especially because of the relative simplicity of their setting work, and their effectiveness against an unprepared target. These attacks can cause significant financial losses by the service interruption or indirectly, by the damage to the image of the target. They target a wide variety of important resources, from banks to news websites, and present a major challenge to making sure people can publish and access important information.

Jie He and al. [7] designed a novel IaaS user oriented 3-dimensional intrusion detection system (3D-IDS) based on the three types of evidences, namely system log, host behavior and network behavior. 3D-IDS are composed of a server and multiple agents. Each agent of 3D-IDS is composed of log collection module, host behavior collection module, network behavior collection module and communication module. Through a distributed collection of information on virtual machines, such as system logs, host behaviors and network behaviors, the system can combine information relevant to provide detailed security situation of each virtual machine for IaaS users.

*Account Hijacking*

Hijacking is the practice of hijack type attacks like account hijacking. Account hijacking takes place when an attacker makes a false authentication account to access of sensitive data or computer account or any account with access to computer equipment. The hijacking involves the modification of strength some settings or behaviors of a computer component. A strong SLA can also be used to protect the Account Hijacking.

### C. Human Threat Malicious Insiders

Malicious insider is people who work for a cloud provider or a business and who has access to data without authorization (or with permission) and used them for personal purpose or profit. This person may be, the IT manager (or network cloud), an employee of another company department, hackers.

According to CERN [8], “A malicious insider is a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems.”

Many research has been developed to identify attacks like malicious insider, as mentioned in [9] by Bruce Schneier, 1999 who proposed a model based on Attack Trees, that is based on varying attacks. Attack Tree offers a formal, methodical way of describing the security of a system. The attacks against a system are represented in a tree structure, with the goal as the root node and different ways of achieving the goal as leaf nodes. Attack tree is as a formal methodology for analyzing the security of systems and subsystems. Attack Tree can assist organizations establish attack circumstances by analyzing system vulnerabilities and dependencies among these vulnerabilities. To detect insider attacks, several studies were based on the attack tree or attack graph.

Ray I., Nayot P [10] proposed a model using Attacks Trees to Identify Malicious Attacks from Authorized Insiders, that model is different from classical intrusion detection systems. It works as an early warning system. He continuously provides the system administrator an estimator of attack probability. Thus he cannot associate a rate of false positives or negatives with this technique. The goal is to ensure that the system enters an alert mode once the probability of an attack is determined to be sufficiently strong. The notion of “sufficiently strong” is based on perceived risks. In the alert state, the following actions will be undertaken to ensure the survivability of information in case of an actual attack.

Many companies, are victims of attack in cloud computing; according to Cloud Security Alliance (CSA) [16] and other some report have been .Assume, as shown in figure 2.

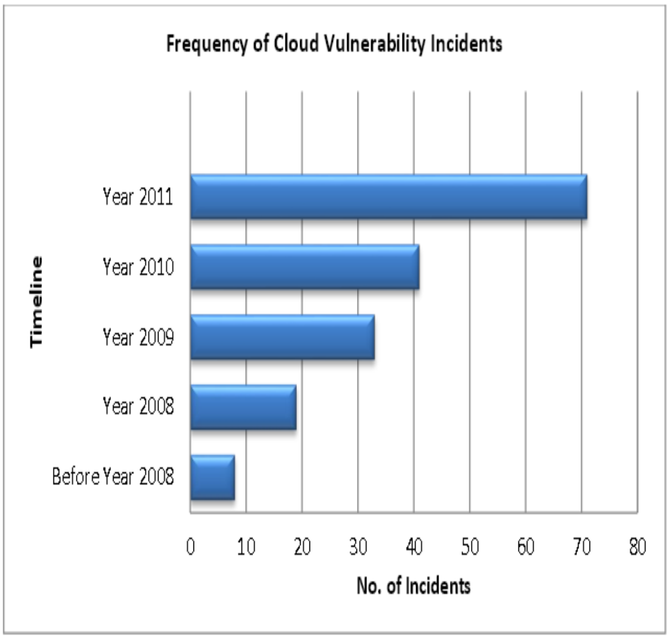

Figure 2: Frequency of cloud vulnerability incidents [15].

In fact from 2009 to 2011 the number of cloud vulnerability incidents more than doubled from 33 to 71, most likely due to the phenomenal growth in cloud services.

## III. CLOUD COMPUTING CHALLENGES

With the advance of technology and especially in the field of cloud computing several researchers and scientific organization were trying to develop techniques to help secure the cloud computing. However there are many sorts of challenges in cloud computing like networks security storage; processing power database/software availability.

Based on a survey conducted by IDC in 2008, the major challenges that prevent Cloud Computing from being adopted are recognized by organizations are as follows:

### *A. Security*

The cloud computing is now presented as a satisfactory answer to the storage and data calculation problem encountered by entreprises.la security in the cloud is an important challenges related to the adoption of cloud computing by enterprises and users although it is a satisfactory answer to the problem of storage and computing data encountered by companies. Users are hesitant the idea to host their data on remote servers or use a shared server. Many problems related to security such as phishing, data breaches, are challenges that cloud service providers.[11]

### *B. Costing model*

Cloud consumers must consider the tradeoffs amongst computation, communication, and integration. Cloud computing is the fact of using the computing power of remote servers and storage to maximize users profits. The cloud is also characterized by its flexibility and adaptation based material needs of users. Indeed this feature is very important because it provides flexibility to price the user pays only as you use. We have several cloud services, the main ones SAAS, PAAS and IAAS and models, allowing the user to make choices are based on its needs. However different services and models; returns us to ask the question: Is it also cheaper to migrate its infrastructure in the cloud by what the different prices offered by cloud providers hides a much more complex problem that does not reflect the characteristic of cloud computing that states that the user only pays for what he consumes. The hybrid models causes some migration problem (hardware and software) by what it augment the computing power and augment the cost of migration infrastructure. In short we can say that while cloud computing offers infrastructure migration flexibility and cost, depending on the model chosen. [11]

### *C. Charging Model*

The elastic resource pool has made the cost analysis a lot more complicated than regular data centers, indeed this feature is very important because it provides flexibility to price the user pays only as you use. Moreover cloud computing: has a hand function to use virtual machine and web browser to access has his data. The SaaS model offered by cloud providers offer a hosting mutualize service related has a significant cost to users and their offering can be very substantial. Therefore, SaaS vendors must balance the tradeoff between providing multi-tenancy and the savings produced by the multi-location such as reducing overheads by depreciation, reducing the number of on-site software licenses, etc. In fact, a strategic and viable billing model with SaaS providers is crucial for the profitability and viability of SaaS cloud providers. [11]

### *D. Service Level Agreement (SLA)*

Users are hesitant to the idea of hosting their infrastructure and data on remote servers, several problems related to data security have led providers cloud providers undertakes to offer a common solution to different cloud models. Service Level Agreement (SLA) is a document that contractually defines the quality of service to expect. In other words this document describes the quality of the proposed service, the hosting period; that offers a cloud provider to keep inform the customer and guarantee confidentiality of its data [12].

### *E. What to Migrate*

Based on a survey (Sample size = 244) conducted by IDC in 2008, the seven IT systems/applications being migrated to the cloud are: IT Management Applications (26.2%), Collaborative Applications (25.4%), Personal Applications (25%), Business Applications (23.4%), Applications Development and Deployment (16.8%), Server Capacity (15.6%), and Storage Capacity (15.5%). These statistical data reveal that income security is an important for companies when they move their data from one server to another. Indeed for the large volume of data (sensitive) to move, companies are hesitant to use IaaS and SaaS models because the secondary functions are external to cloud. That study conducted by IDC, shows us that in three years, 31.5 % of the organization will migrate their data in the cloud. It also puts emphasis on made that this result is relatively low by collaborative applications (46.3%) today [13].

### *F. Cloud Interoperability Issue*

Every cloud vendors offer flexibility services for the use of the different cloud models and services. However we note the difficulties of migration due to many problems such as the security problems, problems due to the different APIs used by cloud providers and also by companies. We also observe compatibility issues with different cloud vendors and business needs. Is all its difficulties show us that cloud computing still needs to grow and improve for better optimization and use of its services [11].

## IV. CONCLUSION

Cloud Computing is a new technology which provides many benefits like storage capacity, cost reduction, time, processing power and performance effective technology. However it has its own security issue that threatens the organization to adopt the cloud technology.

In our papers we have discussed various and types of threats and solutions forward.

## REFERENCES

[1] Peter Mell and Timothy Grance, 2011. (NIST) Definition of Cloud Computing Special Publication 800-145

[2] Security Guidance for Critical Areas of Focus in Cloud Computing V3.0 (2013).

[3] Hongyao Deng, Long Chen , Min Xiao and Xiuli Song, 2013.An Efficient Encryption and Verification Scheme for Preserving Electronic Evidence in Cloud Computing. Published in Journal of Information and Computational Science (joics), pp: 911-922.

[4] E. Shi, J. Molina , J. Staddon, M. Jakobsson, P. Golle, R. Chow and R. Masuoka, 2009.Controlling data in the cloud: outsourcing computation with-out outsourcing control. In Proceedings of the 2009 ACM workshop on Cloud computing security. ACM: pp 85–90.

[5] Pasquale Puzio, Refik Molva, Melek Onen and Sergio Loureiro 2014.Block-level De-duplication with Encrypt Data. Published in Open journal of Cloud Computing(OJCC),volume 1, issue 1.

[6] H. Tsuda, R. Masuoka, T. Takebayashi and T. Hasebe, and 2010. Data loss prevention technologies. Fujitsu Scientific and Technical Journal, vol. 46,no. 1: 47–55.

[7] Jie He, Chuan Tang, Yuexiang Yang, Yong Qiao (2012)"a three-dimensional intrusion detection system (3D-IDS) .IEEE International Conference pp : 12–15.

[8] www.cert.org/insider-threat.

[9] Schneier, Bruce (1999). Attack Trees. SANS Network Security 99, New Orleans, LA

[10] Indrajit Ray, Nayot Poolsappasit and Rinku Dewri 2007. Optimal security hardening using multi- objective optimization on attack tree models of networks.ACM Association for Computing Machinery, CCS'07 Proceedings of the 14th ACM conference on Computer and communications security.pp:204–213.

[11] S. Ramgovind, M. M. Eloff, E. Smith 2010. The Management of Security in Cloud Computing. In PROC 2010 IEEE, International Conference on Cloud Computing.

[12] F. Gens. (2009, Feb).New IDC IT Cloud Services Survey: Top Benefits and Challenges, IDC exchange, Feb. 18, 2011.

[13] C. Weinhardt, A. Anandasivam, B. Blau, and J. Stosser (2009).Business Models in the Service World. IT Professional, vol. 11: 28-33.

[14] . cloud-basedlms-etec522.weebly.com/security.html

[15] Ryan K L Ko, Stephen G Lee, V Rajan, 2013.Cloud Computing Vulnerability Incidents.