IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 01-04
www.iosrjournals.org

Cloud Computing Threats & Their Impact

Sabah Naseem[1], Prof. A B Sasankar[2]

[1]Institute of Science, NagpurR.T. Road, Civil Lines,
Nagpur-440001(Maharashtra)
[2]G. H. Raisoni College of Information Technology,
NagpurHingna, Nagpur-440001(Maharashtra)
snaseem19@gmail.com[1],ashish_sasankar@yahoo.com[2]

Abstract: *We know that now a days the cloud computing is growing more fastly. It is aadvance technology. Where data, hardware & software are shared over a network on use & pay rule. Because of this many organization are moving towards the cloud. There is no. of threats which cause possible harm or used to exploit important data. A threat can be either intentional or accidental. In this paper we will discuss about the threat & security issues. What are the different type of threats & their impact.*

Keywords: *cloud computing , cloud computing service model, threats.*

I. INTRDUCTION

Cloud computing is the use of computing resources i.e hardware and software that are delivered over a network or internate. In this cloud computing user can access hardware, software & infrastructure at low cost.Cloud computing is a flexible and cost effective for consumer or business. More large & small companies and organizations are adopting this cloud . There are different types of cloud i.e public, private,community and hybrid which we will discuss below. Cloud computing is based on different services over a network like software- as- a-service(Saas) , Platform-as- a-service(Paas) & Infrastructure-as –a-service(Iaas). Before starting the journey to cloud, organizations must considers the possible threats and vulnerabilities that may convert their dreams of enhancing scalability and saving management cost into a nightmare of data loss and misuse. in other words this technology is not trustworthy as it is affected with threats and vulnerabilities. We have termed a cloud with threats and vulnerabilities as a stormy cloud. Based on Cloud Security Alliance (CSA) and our research [1]. The identified threats and their impacts we will discuss in this paper.

II. TYPES OF CLOUD COMPUTING

Many Organizations deal with the storing and retrieving of huge data and cloud computing helps in performing it efficiently with minimum cost, time and maximum flexibility. Besides the benefits associated with the cloud computing, there are different security issues organization has to deal with inorder to separate one cloud users data from the other inorder to maintain confidentiality/privacy, reliability and integrity (Bugiel, Nurnberger, Sadeghi, & Schneider, 2011).

- **PUBLIC CLOUD:**

It is a part of cloud computing.In this cloud computing every local user can access the cloud. User can easily access this cloud on pay-and-usage.In this cloud general user can access web browser, web application & resources etc.The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services [2].

- **PRIVATE CLOUD:**

It is also a part of cloud computing.A single organization or companies make their own private cloud in which the employee or member or authorized person of that organization or companies can access this cloud. Unauthorised user can’t access. This cloud consists on the hosting of private applications, storage, or computation in the same company emulating a cloud in Internet but only for private use (private networks) [3].

- **HYBRID CLOUD:**

Hybrid cloud is a combination of public and private cloud. A hybrid cloud is typically offered in one of two ways: a vendor has a private cloud and forms a partnership with a public cloud provider, or a public cloud provider forms a partnership with a vendor that provides private cloud platforms[4].

- **COMMUNITY CLOUD:**

In community cloud computing more than one public cloud, private cloud or hybrid clouds are merged together. We can say that it is a combination of one or more cloud. This community cloud shared by many organization for a single purpose**.**

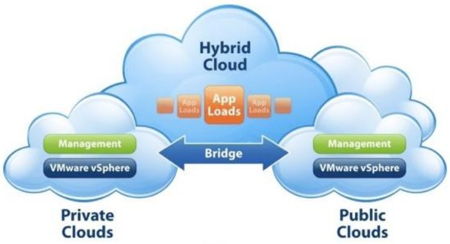

Fig-1: types of cloud[5]

III. CLOUD COMPUTING SERVICES

Cloud computing is based on different basic model. Software-as-a-service(Saas), Platform-as-a-service(Paas), Infrastructure-as-a-service(Iaas).

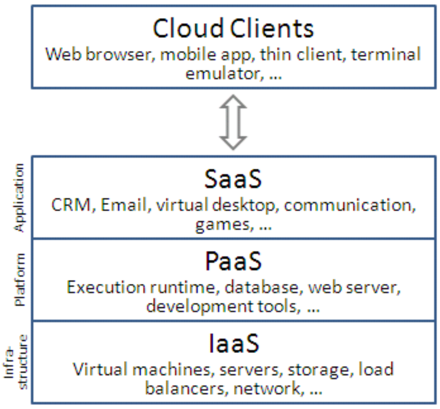
Cloud Clients
Web browser, mobile app, thin client, terminal emulator, ...
Application
SaaS
CRM, Email, virtual desktop, communication, games, ...
Platform
PaaS
Execution runtime, database, web server, development tools, ...
Infra-structure
IaaS
Virtual machines, servers, storage, load balancers, network, ...

Fig-2 : Architechture for service model[6]

- **Saas(SOFTWARE-AS-A-SERVICE):**

In the SaaS model, cloud providers install and operate application software in the cloud and cloud users access the software from cloud clients. The cloud users do not manage the cloud infrastructure and platform on which the application is running. This eliminates the need to install and run the application on the cloud user's own computers simplifying maintenance and support[7].

- **Paas(PLATFORM_AS_A_SERVICE):**

In Platform-as-a-service user can easily access the hardware, software, operating system and programming language without purchasing. In cloud user can use these things on its own machine by the help of this service.

- **Iaas(INFRASTRUCTURE_AS_A_SERVICE):**

IaaS (Infrastructure as a Service) is a cloud computing category and a provision model in which a company outsources the physical equipment used to support operation, including storage, hardware, servers and networking components. In this model, the cloud user is usually responsible for patching and maintaining the operating systems and application software unless you are working with an Enterprise provider that offers Managed Services in their IaaS environment.

IV. CLOUD COMPUTING THREATS

A) Abuse & Nefarious use of cloud computing

Many a times the Cloud Computing service providers do not have strict registration process. Using a credit card any one can register for cloud computing services online or many vendors offer free trial of their services. This opens an avenue for many nefarious users, who could anonymously exploit the cloud computing resources for malicious purpose like setting up botnets, spamming, spreading virus / malwares etc.The attacker could attempt

- Password and key cracking
- DDOS
- Launching dynamic attack points
- Hosting malicious data
- Botnet command and control
- CAPTCHA solving[8]

IMPACT:Criminals continue to leverage new technologies to improve their reach, avoid detection, and improve the effectiveness of their activities. Cloud Computing providers are actively being targeted, partially because their relatively weak registration systems facilitate anonymity, and providers' fraud detection capabilities are limited.

B)Malicious Insider

The threat of a malicious insider is well-known to most organizations.This threat is amplified for consumers of cloud services by the convergence of IT services and customers under a single management domain, combined with a general lack of transparency into provider process and procedure. For example, a provider may not reveal how it grants employees access to physical and virtual assets, how it monitors these employees, or how it analyzes and reports on policy compliance.It also includes,

- Particularly poignant for cloud computing
- Little risk of exposure
- System administrator qualifications and inspection process for cloud services provider may be different that of the data owner[9]

IMPACT :Human risk is the worst of all specially in the cloud computing environment where there is no control on the people handling & managing your data. A malicious insider could lead to compromise of confidentiality, availability & integrity which are the pillars of Information Security. This could further lead to legal and regulatory implications[10]

B) Data loss or Leakage

There are so many ways in which user can destroy the data. Some of the causes could be malicious insiders, sharing of data between employees, improper & irregular backups, inappropriate data retention policy, users forgetting the secret keys / passwords etc.Deletion or alteration of records without a backup of the original content is an obvious example. It also includes

- Data is outside the owner's control
- Data can be deleted or decoupled (lost)
- Encryption keys can be lost
- Unauthorized parties may gain access
- Caused by

✓ Insufficient authentication, authorization, and access controls
✓ Persistence and remanance
✓ Poor disposal procedures
✓ Poor data center reliability

IMPACT: Loss of core intellectual property could have competitive and financial implications. Worse still, depending upon the data that is lost or leaked, there might be compliance violations and legal ramifications.

V. CONCLUSION

Here we discussed about technology of cloud computing. Explain its definition,service models, deployment models and some existing security threats. We know that the cloud computing is the development trend in the future. Cloud computing brings us almost infinite computingcapability, good scalability, service on-demand, pay per use and so on, also challenger at security privacy, legal issues and so on. Cloud computing offers many benefits, but it also is vulnerable to threats. As the uses of cloud computing increase, it is highly likely that more criminals will try to find new ways to exploit vulnerabilities in the system. There are manyunderlying challenges and risks in cloud computing that increase the threat of data being compromised. Security concerns must be addressed in order to establish trust in cloud computing technology.Here we are dealing with three types of threat and impact to find there solutions.

REFERENCES

[1]. MervatAdibBamiah* et al. / (IJAEST) INTERNATIONAL JOURNAL OF ADVANCED ENGINEERING SCIENCES AND TECHNOLOGIES Vol No. 9, Issue No. 1, 087 – 090

[2]. Che Wan AmiruddinChek Wan Samsudin,Data Provenance for e-Social Science Cloud Applications

[3]. Albert Folch, Interface development for Eucalyptus based cloud

[4]. http://searchcloudcomputing.techtarget.com/definition/hybrid-cloud

[5]. http://talkcloudcomputing.com/wp-content/uploads/2012/10/Cloud-Computing-2-Web-1.jpg

[6]. Cloud Computing: Security Threats and Counter Measures, K.ValliMadhavi,R.Tamilkodi 2, K.JayaSudha 3, Department of Computer Applications, Department of EXTC, GIET, Rajahmundry3SFIT, Mumbai vallimb@yahoo.comtamil_kodiin@yahoo.co.in

[7]. Hamdaqa, Mohammad. A Reference Model for Developing Cloud Applications.http://www.stargroup.uwaterloo.ca/~mhamdaqa/publications/A%20REFERENCEMODELFORDEVELOPINGCLOUD%20APPLICATIONS.

[8]. William R. Claycomb, PhD. Lead Research Scientist CERT Enterprise Threat and Vulnerability Management Team

[9]. Cloud Computing Security, William R. Claycomb

[10]. Google,Cloud Security & Threat

[11]. Cloud security alliance,Top Threats to Cloud Computing V1.0 Prepared by the Cloud Security Alliance March 2010