Cloud Computing: Threats and Security

Deepti Singh Kshatriya
Department Of Computer Science & IT
Kamla Nehru Mahavidyalaya
Korba(C.G), India

Manju Vishakh Nair
Department Of Computer Science & IT
Kamla Nehru Mahavidyalaya
Korba(C.G), India

***Abstract*—Cloud computing is one of today's most exciting technologies due to its ability to reduce costs associated with computing while increasing flexibility and scalability for computer processes. During the past few years, cloud computing has grown from being a promising business idea to one of the fastest growing parts of the IT industry. IT organizations have expresses concern about critical issues (such as security) that exist with the widespread implementation of cloud computing. Cloud computing is a promising technology to facilitate development of large-scale, on-demand, flexible computing infrastructures. But without security embedded into innovative technology that supports cloud computing, businesses are setting themselves up for a fall. The trend of frequently adopting this technology by the organizations automatically introduced new risk on top of existing risk. Obviously putting everything into a single box i.e. into the cloud will only make it easier for hacker.**

Cloud computing is the delivery of computing services over the Internet. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. Examples of cloud services include online file storage, social networking sites, webmail, and online business applications. The cloud computing model allows access to information and computer resources from anywhere that a network connection is available. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications. Those resources can include applications and services, as well as the infrastructure on which they operate.

By deploying IT infrastructure and services over the network, an organization can purchase these resources on an as-needed basis and avoid the capital costs of software and hardware. With cloud computing, IT capacity can be adjusted quickly and easily to accommodate changes in demand. While remotely hosted, managed services have long been a part of the IT landscape, a heightened interest in cloud computing is being fueled by ubiquitous networks, maturing standards, the rise of hardware and software virtualization, and the push to make IT costs variable and transparent.

In the last few years, cloud computing has grown from being a promising business concept to one of the fastest growing segments of the IT industry. Now, recession-hit companies are increasingly realizing that simply by tapping into the cloud they can gain fast access to best-of-breed business applications or drastically boost their infrastructure resources, all at negligible cost.

Security, in particular, is one of the most argued-about issues in the cloud computing field; several enterprises look at cloud computing warily due to projected security risks. The risks of compromised security and privacy may be lower overall, however, with cloud computing than they would be if the data were to be stored on individual machines instead of in a so called "cloud".

Keywords- Cloud Computing; Service Model; Deployment Model; Security; Threats;

I. INTRODUCTION

Cloud Computing: - Cloud Computing is a flexible, cost-effective, and proven delivery platform for providing business or consumer IT and hardware. With cloud computing, IT capacities can services over the Internet. As opposed to hosting and operating those resources locally, such as on a college or university network. Those resources can include applications and services, as well as the infrastructure on which they operate. By deploying IT infrastructure and services over the network, an organization can purchase these resources on an as-needed basis and avoid the capital costs of software be adjusted quickly and easily to ac-accommodate changes in 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.

CA Technologies and Ponemon Institute surveyed 103 cloud service providers in the US and 24 in six European countries for a total of 127 separate providers. Respondents from cloud provider organizations say SaaS (55 %)is the most frequently offered cloud service, followed by IaaS (34 %) and PaaS (11 %). 65% of cloud providers in this study deploy their IT resources in the public cloud environment, 18 % deploy in the private cloud and 18 % are hybrid.

Purpose and Scope of this Research Paper

This paper presents an overview and the study of the cloud computing threats & security and the future trends of cloud computing. Cloud computing has been on the rise for many years but the threats to this technology are now more tangible than ever. If the industry is to be legitimized by the concerned citizen it must first overcome a serious of potential threats, beyond just cybercrime.

In this development, we closely watch cloud computing security on a very technical level, focusing primarily on attacks and hacking attempts related to cloud computing providers and systems. We pointed out lately, the specific security threats and vulnerabilities of services and service-oriented architectures require new security criteria, so do attacks on cloud computing scenarios. In this work-in-progress paper, we try to anticipate the classes of security issues that will arise from the cloud computing paradigm, and we give preliminary some solution for these, based on the notion of attack surfaces.

Explain:

The question focus was to identify the most relevant issues in Cloud Computing which consider threats and solutions of security for Cloud Computing. This question had to be related

with the aim of this work; that is to identify and relate vulnerabilities and threats with possible solutions. Therefore, the research question addressed by our research was the following: What security vulnerabilities and threats are the most important in Cloud Computing which have to be studied in depth with the purpose of handling them?

II. SERVICE MODELS

Software as a Service (SaaS). The capability provided to the consumer is running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying

Cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Cloud Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

Cloud Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

III. DEPLOYMENT MODELS

Private cloud: The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.

Community cloud: The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

Public cloud: The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

Hybrid cloud: The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

IV. THREATS OF CLOUD COMPUTING

Threat .1: Data Breaches

One of the top threats to cloud computing is data breaches. All the computer systems connected to the Internet can be accessed by virtually any person. This exposes cloud computing service providers to the threat of skilled hackers with malicious intentions. In 2013 the number of reported cases of server breaches was over 300 and they resulted in the loss of about10 million data records. More and more breaches are expected as the number of national (and international, as we've witnessed with China) underground hacking communities continues to grow.

Threat .2: Data Loss

Another serious threat stems from cloud computing service providers potential inability to prevent data loss. In our plugged in world, most people know that loss of data is inevitable at one point or another. However, this threat is compounded by the sheer amount of data handled by cloud computing service providers. There is increasing amount of sensitive data relayed to cloud computing firms and this data could get lost in any number of ways, including through accidental deletion or corruption.

Threat .3: Account Hijacking

Hijacking of accounts at cloud computing companies is another potentially serious threat. It is usually possible for authorized company personnel to remotely access cloud data via mobile devices or remote computers. "The potential for account hijacking, or data hijacking, increases when employees are accessing sensitive information via remote platforms that don't necessarily have the security mechanisms in place that would otherwise exist at a workstation computer".

Threat .4: Insecure application programming interfaces (APIs)

Insecure Application Programming Interfaces (APIs) are another threat to cloud computing. These interfaces offer ways for programs to communicate with each other and their security is not always completely guaranteed. The loopholes in security might grant people with malicious intentions access to sensitive information passing through the communication channel.

Threat .5: Denial of Service

Although it doesn't gravely affect integrity of the data stored in cloud computing servers, denial of service can temporarily deny access of data to legitimate users.

Threat .6: Data Handling

Sharing of technology and resources among different organizations always poses a risk to the data being handled. Sometimes servers at cloud computing firms are configured to work with data from few clients. Once data from a client with different requirements is added to the system, there are many things that may go wrong.

V. SOLUTION FOR SECURITY ISSUES IN CLOUD COMPUTING

1. **Services for Security:** Cloud service delivery models are Software as a Service (SaaS), Platform as a Service

(PaaS) and Infrastructure as a Service (IaaS) for provide security region. This will be protect private information before sending to cloud and also protect our API keys.

2. **Data segregation & Recovery:** Make sure that encryption is available at all stages, and that these encryption schemes were designed and tested by experienced professionals. Even if we don't know where our data is, a cloud provider should tell us what will happen to our data and service in case of a disaster. Any offering that does not replicate the data and application infrastructure across multiple sites is vulnerable to a total failure. We can ask our provider if it has "the ability to do a complete restoration, and how long it will take."
3. **Data security:** Security will need to move to the data level so that enterprises can be sure their data is protected wherever it goes. For example, with data-level security, the enterprise can specify that this data is not allowed to go outside of the European Union. It can also force encryption of certain types of data, and permit only specified users to access the data.
4. **Application security:** This is where the security features and requirements are defined and application security test results are reviewed. Application security processes, secure coding guidelines, training, and testing scripts and tools are typically a collaborative effort between the security and the development teams. Although product engineering will likely focus on the application layer, the security design of the application itself, and the infrastructure layers interacting with the application, the security team should provide the security requirements for the product development engineers to implement.
5. The purpose of both studies is to learn how users and providers of cloud computing applications, infrastructure and platforms are addressing the need to safeguard information in the cloud. Cloud computing has been defined as the use of a collection of distributed services, applications, information and infrastructure comprised of pools of computer, network, information and storage resources. These components can be rapidly orchestrated, provisioned, implemented and decommissioned using an on-demand utility-like model of allocation and consumption.
6. To address the security issues listed above, SaaS providers will need to incorporate and enhance security practices used by the managed service providers and develop new ones as the cloud computing environment evolves.

VI. Conclusion And Future Work

Cloud computing is the future of IT industries. It helps the industries to get efficient use of their IT Hardware and Software resources at low cost. On one hand, the security-sensitive applications of a Cloud computing require high degree of security on the other hand, cloud computing are inherently vulnerable to security attacks. Therefore, there is a need to make them more secure and robust to adapt to the demanding requirements of these networks.

If you are considering using the cloud, be certain that you identify what information you will be putting out in the cloud, which will have access to that information, and what you will need to make sure it is protected. Additionally, know your options in terms of what type of cloud will be best for your needs, what type of provider will be most useful to you, and what the reputation and responsibilities of the providers you are considering are before you sign up.

The future of cloud computing is really appealing, giving the vision of cheap communications. At present, the general trend in cloud computing is toward mesh architecture and large scale. Improvement in bandwidth and capacity is required, which implies the need for a higher frequency and better spatial spectral reuse. Large scale cloud computing is another challenging issue in the near future which can be already foreseen.

References

[1] Ricardo vilaca, Rui oliveira 2009. Clouder : A Flexible Large Scale Decentrali- zed Object Store. Architecture Overview. Proceeding of WDDDM ’09
[2] Michael Miller. 2009. Cloud Computing-Web Based Application that change the way you collaborate online. Publishing of QUE, 2nd print.
[3] National Institute Of Standard and technology csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc, 2009
[4] Open Security Architecture http:/ /www. Open securityarchitecture.org/
[5] Tim Mather, Subra Kumaraswamy, Shahed Latif Cloud Security and Privacy : An Enterprise perspective of Risks
[6] GregBoss, Padma Malladi, Dennis Quan, Linda Legregni and Harold hall 2007. Cloud Computing.Available from www.ibm.com/developerworks/websphere/zones/hipods/.
[7] Anthony T.Velte, Toby J.Velte and Robert Elsenpeter 2010. Cloud Computing- A Practical Approach. Publishing of Tata McGRAW Hil.
[8] Nils Gruschka and Meiko Jensen, “Attack Surfaces: A Taxonomy for Attacks on Cloud Services”.IEEE rd International Confrence on Cloud Computing,2010.
M. Casassa-Mont, S. Pearson and P. Bramhall, “Towards Accountable Management of Identity and Privacy: Sticky policies and Enforceable Tracing Services”, Proc. DEXA 2003, IEEE Computer Society, 2003, pp. 377-382