Cloud Computing: Threat’s in Business Data Security

Suraj Kumar Sahu1, Pradeep Kumar Mahapatro2
1Department of Computer Science & Engineering, Centurion University of Technology and Management, Odisha, INDIA
2Assistant Professor, Department of Computer Science & Engineering, Centurion University of Technology and Management, Odisha, INDIA

ABSTRACT
Cloud computing is Internet-based computing, whereby shared resources, software, and information are provided to computers and other devices on demand, as with the electricity grid. It is a completely internet dependent technology where client data is stored and maintain in the data center of a cloud provider. In this paper, we aim to pinpoint the challenges and issues of cloud computing. Regardless of its advantages, the transition to this computing paradigm raises security concerns, which are the subject of several studies. With the introduction of numerous cloud based services and geographically dispersed cloud service providers, sensitive information of different entities is normally stored in remote servers and locations with the possibilities of being exposed to unwanted parties in situations where the cloud servers storing that information are compromised. including authentication, encryption and decryption and compression. In this paper, the authors discuss security issues, privacy and control issues, accessibility issues, confidentiality, integrity of data and many more for cloud computing.

Keywords--- PaaS, Security, Cloud

I. INTRODUCTION
Cloud computing is defined as provision of resources, application and information as a service over the cloud on demand. In a cloud based computing infrastructure, the resources are normally in someone else’s premise or network and access remotely by the cloud users. Today small and medium size companies are moving to Cloud due to various reason like reduced hardware, maintenance cost pay-for use, scalability, accessible location independent, on-demand security controls, fast deployment, flexibility and the highly automated process i.e. he customer need not worry about software up-gradation. Though cloud computing is targeted to provide better utilization of resources using virtualization techniques and to take up much of the work load from the client, it is fraught with security risks.

1. Cloud Models
   • Delivery Models
     – SaaS:
     • Software as a Service is nothing but a software distribution model which are made available to customers over a network such as server or Internet the example of SaaS is Google Apps, Cisco’s WebEx, Salesforce CRM.
     – PaaS:
     • The offering also includes a software execution environment. As for example, there could be a PaaS application server that enables the lone developers to deploy web-based applicationsthe examples of PaaS are database, webservers, development tools.
     – IaaS:
     • Refers to the sharing of hardware resources for executing services, typically using Virtualization technology. Infrastructure as a Service is an equipment which is used to support hardware, software, storage, servers and mainly used for delivering software application environments the examples of IaaS are Amazon, Microsoft, VMWare and Red Hat.

• Deployment Models
  – Private cloud
  – Community cloud
  – Public cloud
  – Hybrid cloud
• We propose one more Model: Management Models (trust and tenancy issues)
  – Self-managed
  – 3rd party managed (e.g. public clouds and VPC)
II. SECURITY ISSUES FOR CLOUDS

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. Privacy is important for organizations, especially when individual’s personal information or sensitive information is being stored but it is not yet completely understood whether the cloud computing infrastructure will be able support the storing of sensitive information without making organizations liable from breaking privacy regulations.

2.1. Data integrity:
In cloud, at the same time, many cloud providers and consumers can access and modify the data. So, there is a loss of data integrity in the cloud computing.

2.2. Data loss:
Sensitive information is disclosed to the unauthorized users that are not authorized to see the data. At that time, there was a possibility of data breaches.

In cloud computing administrative access must be conducted via the Internet, increasing exposure and risk. It is extremely important to restrict administrative access to data and monitor this access to maintain visibility of changes in system control. Data access issue is mainly related to security policies provided to the users while accessing the data. Location transparency is one of the prominent flexibilities for cloud computing, which is a security threat at the same time – without knowing the specific location of data storage, the provision of data protection act for some region might be severely affected and violated. Cloud users’ personal data security is thus a crucial concern in a cloud computing environment.

III. WHY IS CLOUD SECURITY IMPORTANT?

Thus, in cloud computing context, a security concern is always some type of risk but any risk cannot be blindly judged to be a security concern. Allocation of responsibilities among the parties involved in a cloud computing infrastructure might result in experiencing inconsistency which might eventually lead to a situation with security vulnerabilities.

- Increasing Usage of Cloud Services in Non-traditional Sectors
- Growing Adoption of Cloud Services in Government Departments
- Rise in Cloud Service-specific Attacks
- Growing Usage of Cloud Services for Critical Data Storage
- Rise in Employee Mobility

IV. SECURITY PRINCIPLES

4.1. Confidentiality
Confidentiality means keeping user’s data secret in the Cloud systems. Cloud Computing system offerings (e.g. Applications and its infrastructures) are essentially public networks Therefore, keeping all confidential data of users’ secret in the Cloud is a fundamental requirement which will attract even more users consequently.

4.2. Integrity
The concept of cloud information integrity is based on two principles Prevention of modification of data from unauthorized users and preventing the unauthorized modification of data by authorized user.

4.3. Security on provider level
Provider need to check that the server is secured from the external threats. A cloud is good if there is a security offered by the provider to the customers.

4.4. Security on user level
User needs to check that the data received by the provider are without any loss.

V. TAXONOMY OF FEAR

- Difficult to audit data held outside organization in a cloud
- Forensics also made difficult since now clients don’t maintain data locally
- Legal quagmire and transitive trust issues
- Who is responsible for complying with regulations?
  e.g.: SOX, HIPAA, GLBA
- If cloud provider subcontracts to third party clouds, will the data still be secure?

VI. CLOUD SECURITY RISKS

The security risks associated with each cloud delivery model vary and are dependent on a wide range of factors including the sensitivity of information assets, cloud architectures and security control involved in a particular cloud environment. In the following we discuss these risks in a general context, except where a specific reference to the cloud delivery model is made.

6.1. Risks for Cloud Service Users
- Responsibility Ambiguity
- Unsecure Cloud Service User Access
- Lack of Information/Asset Management
- Data loss and leakage

6.2. Risks for Cloud Service Providers
- Responsibility Ambiguity
- Protection Inconsistency
- Evolutional Risks
- Unsecure Administration API
- Shared Environment
6.3. New Vulnerabilities & Attacks

- Threats arise from other consumers
- Due to the subtleties of how physical resources can be transparently shared between VMs
- Such attacks are based on placement and extraction
- A customer VM and its adversary can be assigned to the same physical server
- Adversary can penetrate the VM and violate customer confidentiality

VII. SOLUTION TO THE SECURITY PROBLEMS

7.1. Denial of Service attack solution

DOS attack is prevented by using prior automatic switches that provide the packet rate analysis. DOS attack is mainly used to protect the network traffic against authorized and unauthorized users.

7.2. Malware injection Solution

The malware-injection attack is prevented by allowing the cloud users to create an account in the cloud and provider create the copy of cloud user’s VM image in the cloud image storage system.

7.3. Data Encryption

Encryption is a key technology for data security. Understand data in motion and data at rest encryption. Remember, security can range from simple (easy to manage, low cost and quite frankly, not very secure) all the way to highly secure (very complex, expensive to manage, and quite limiting in terms of access). You and the provider of your Cloud computing solution have many decisions and options to consider.

7.4. Creating Cloud Domains

- Security, Business Continuity, Disaster Recovery
- Data Center Operations
- Incident Response Issues
- Application Security
- Encryption & Key Mgt
- Identity & Access Mgt

7.5. Minimize Lack of Trust

- Policy Language
- Certification

7.6. Minimize Loss of Control

- Monitoring
- Utilizing different clouds
- Access control management
- Identity Management (IDM)

VIII. CONCLUSION

Cloud computing has enormous prospects, but the security threats embedded in cloud computing approach are directly proportional to its offered advantages. Security concerns are an active area of research and experimentation. Lots of research is going on to address the issues like network security, data protection, virtualization and isolation of resources. Cloud service providers need to inform their customers on the level of security that they provide on their cloud. Although Cloud computing can be seen as a new phenomenon which is set to revolutionize the way we use the Internet, there is much to be cautious about. There are many new technologies emerging at a rapid rate, each with technological advancements and with the potential of making human’s lives easier. However, one must be very careful to understand the security risks and challenges posed in utilizing these technologies.

REFERENCES


Copyright © 2016. Vandana Publications. All Rights Reserved.