International Journal of Allied Practice, Research and Review
Website: www.ijaprr.com (ISSN 2350-1294)

Cloud Computing: Unexampled firmness of purpose of Java Technologies as for Security vulnerabilities and Cloud user's Interaction on the Web.

[1] Dr. Tejinder Singh
Assistant Professor of Computer Science and Deputy Dean IRP, Baba Farid College,
Bathinda, Email: - tejinder31.singh@gmail.com

Abstract - Here in this paper, we explore comparative study to analyze the cloud computing with the use of Java Technologies. Cloud computing is a natural firmness of purpose for data and computation centers with automated systems management, workload balancing, and virtualization technologies. A mounting number of vendors are contribution Java Platform as a Service (PaaS) solutions that support the Java Standard Edition (JSE) and JEE standard. Java EE 7 Provides more or less additional functionality even you can handle the security purpose and applications on the web community. We have seen that Java EE is the major enterprise platform with millions of lines of code available in the data centers, a path to move them to Cloud will be very attractive to enterprises. As a security issues on cloud environment data transfer, data sharing and user permission's which form could be accessed on via cloud computing. Java EE 7 be responsible for regarding data transfer and user permissions. In this paper, the author discuss security issues, privacy and control issues, accessibility issues, confidentiality, integrity of data and many more for cloud computing And discuss, three cloud service models were compared; cloud security risks and threats were investigated based on the nature of the cloud service models.

Keywords: J2EE, Enterprise; Security; Users; Applications

I. Introduction

As presently, java introduces the concept of cloud computing with the Enterprise technology. Java provides the environment for cloud, Service engines provide logic in the environment, such as XSL (Extensible Stylesheet Language) transformation or BPEL (Business Process Execution Language) orchestration. Binding components are sort of "connectors" to external services or applications. They allow communication with various protocols, such as SOAP, REST, Java Message Service, or ebXML. Especially if you mean the enterprise as we know it today. While there are important security, privacy and regulatory issues that enterprises need to sort through before full migration to the cloud, and cloud vendors need to strengthen cloud capabilities in these areas before enterprise applications can be effectively hosted in the cloud, there are benefits that cloud technologies do offer today that can be leveraged in the deployment of many enterprise applications [1]. In simple words, Cloud computing is the combination of a technology, platform that provides hosting and storage service on the Internet. Cloud computing aims to provide scalable and inexpensive on -demand computing infrastructures with good quality of service levels. "A model for enabling convenient, on-demand network access to a shared pool of configurable service delivery models coexist in one cloud platform the security management process [2].

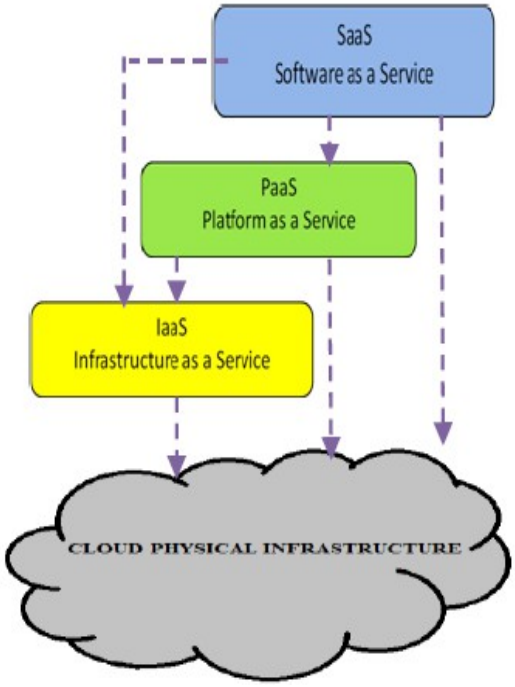

Figure 1: Cloud Service models

II. Cloud Computing Threats

Cloud computing faces just as much security threats that are currently found in the existing computing platforms, networks, intranets, internets in enterprises. These threats, risk vulnerabilities come in various forms. It identified the following seven major threats: [3].

- Abuse and Nefarious Use of Cloud Computing
- Insecure Application Programming Interfaces
- Malicious Insiders
- Shared Technology Vulnerabilities
- Data Loss/Leakage
- Account, Service & Traffic Hijacking
- Unknown Risk Profile

III. Cloud Security

with the security risk and vulnerability in the enterprise cloud computing that are being discovered enterprises that want to proceed with cloud computing should, use the following steps to verify and understand cloud security provided by a cloud provider: [3]

- Understand the cloud
- Demand Transparency
- Reinforce Internal Security
- Consider the Legal Implications
- Pay attention

a. *Issues to Clarify Before Adopting Cloud Computing*

An enterprise cloud computing user should address with cloud computing providers before adopting: [3]

- User Access

- Regulatory Compliance
- Data location
- Data Segregation
- Disaster Recovery Verification
- Disaster Recovery
- Long-term Viability

IV. Data Security on the Cloud Side

From the laaS on the bottom foundation layer to the PaaS on the middle layer and the SaaS on the top layer, cloud storage is always an important key factor for implement the application of cloud computing. lasS layer is supporting the networking service. In the following, some consideration regarding the security issue for device and equipment must be focused.

- Storage and system protection
- Data protection

Encrypt those confidential file or sensitive data before uploading. After then, those encrypted data could be uploading to the storage designated and provided by service provider of the cloud computing through secure channel. The demonstrated operating process is shown [4]

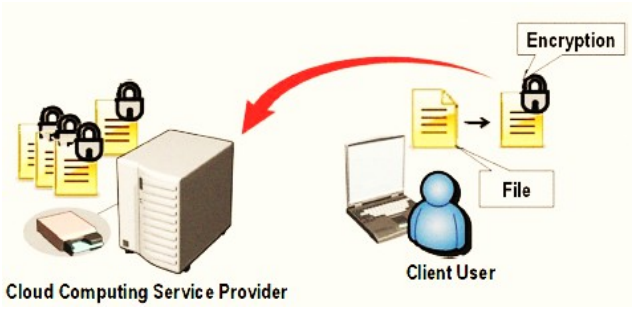

Figure 2: Data Encryption before Uploading

V. Java Vulnerabilities for Cloud

Over the years that the X-Force team has been tracking Security incidents, the overall attack tactics and techniques have not changed significantly. The number of overall incidents has increased, the amount of traffic used in distributed-denial-of-service (DDoS) attacks has multiplied and the number of leaked records has been steadily rising. They successfully exploited vulnerable web applications with attacks such as SQL injection (SQLi) and cross-site scripting (XSS), as well as utilized a mix of sophisticated and generally accessible toolkits to gain critical points of entry. [5]

Figure 3. Most-Commonly Attacked Industries

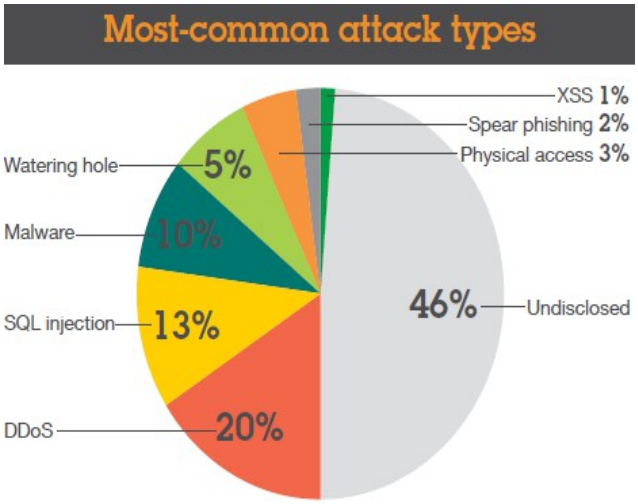

Figure 4. Most-Common Attack Types

An analysis of X-Force threat intelligence data during the month of December, 2013 reveals that out of a survey of more than one million Trusteer banking and enterprise customers, the most targeted applications were Oracle Java, Adobe Reader and popular browsers.[5]

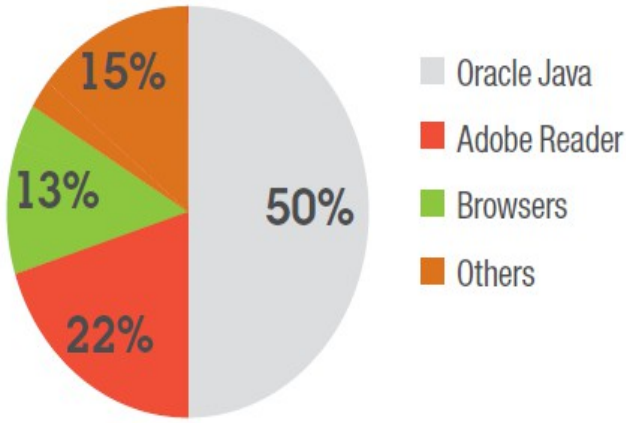

Figure 5. Exploitation of application vulnerabilities

Disclosure comes in the form of two detailed reports

- Weaknesses with the PaaS's implementation and configuration.
- Opportunities for users to access other users' applications, and, most importantly,
  - Issues that could expose the service platform to attacks from remotely executed code.

VI Conclusion

In this paper I have provided some information regarding java Vulnerabilities for cloud web applications and others. I have showing the survey report e-force that it is shown in figures most-common attack types
Cloud security and most common attacked Industries. The advent of cloud computing emphasizes the importance of service availability; in fact, for an increasing number of mission-critical applications, availability becomes subject to contractual obligations. We present evidence that the infrastructure that underlies, and the applications that rely upon, cloud computing undergo a fast-paced evolution.

VII References

[1] "Cloud computing A collection of working papers", Thomas B Winans , John Seely Brown, 2009 Deloitte Development LLC., www.deloitte.com

[2] "Security Issues with Possible Solutions in Cloud Computing-A Survey", Abhinay B.Angadi, Akshata B.Angadi, Karuna C.Gull, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 2, Issue 2, February 2013, ISSN: 2278 – 1323, pp-652-661.

[3] "AN OVERVIEW OF THE SECURITY CONCERNS IN ENTERPRISE CLOUD COMPUTING", Anthony Bisong1 and Syed (Shawon) M. Rahman, International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.1, January 2011, PP-30-45.

[4] "Information Security Issue of Enterprises Adopting the Application of Cloud Computing", Chang-Lung Tsai Uei-Chin Lin Allen Y. Chang Chun-Jung Chen, National Science Council and Chinese Culture University of Taiwan, R.O.C., PP-648-649.

[5] "IBM X-Force Threat Intelligence Quarterly 1Q 2014", IBM Security Systems, February 2014.

[6] "Cloud Software Upgrades: Challenges and Opportunities", Iulian Neamtiu, Department of Computer Science and Engineering University of California, Riverside Email: neamtiu@cs.ucr.edu

[7]" Security Vulnerability Notice" ,SE-2013-01-ORACLE,Security vulnerabilities in Oracle Java Cloud Service, Issues 1-28.