Issues and Challenges of Security in Cloud Computing Environment

Prof. Divyakant Meva
Faculty of Computer Applications, Marwadi Education Foundation's Group of Institute, Rajkot
Email: divyakantmeva16@yahoo.co.in
Dr. C. K. Kumbharana
Head, Department of Computer Science, Saurashtra University, Rajkot
Email: ckkumbharana@yahoo.com

--**ABSTRACT**---

The term cloud computing is a relatively recent vintage. In the year of 2008, this term came in popularity. Since then, this term has emerged a lot within short span of time. As it is known fact of IT industry that every emerging technology brings some issues and challenges, this is also true for Cloud Computing Environment. In this paper, authors have tried to throw some light on above said topic especially on SaaS.

Keywords - **Cloud Computing, Security, SaaS security, issues and challenges**

[1] INTRODUCTION

Though the term Cloud Computing is not new now a day, let us have a definition of Cloud computing:

"Cloud computing is a type of computing that provides simple, on-demand access to pools of highly elastic computing resources. These resources are provided as a service over a network (often the Internet), and are now possible due to a series of innovations across computing technologies, operations, and business models. Cloud enables the consumers of the technology to think of computing as effectively limitless, of minimal cost, and reliable, as well as not be concerned about how it is constructed, how it works, who operates it, or where it is located. [1]"

When we consider Cloud Computing, the following characteristics must be considered:

1. Scalable
2. Elastic
3. Self- service
4. Ubiquitous access
5. Complete virtualization
6. Relative consistency
7. Commodity

The other common characteristics are:

1. Measured service
2. Multiple tenants
3. Multiple applications
4. Scalable (Individual application)
5. Reliable

Cloud can be divided into three major layers namely:

1. Cloud Infrastructure (IaaS)
2. Cloud Application Platform (PaaS)
3. Cloud Application (SaaS)

The first layer contains all physical and virtual resources used to build cloud.

The second layer is responsible to organize and operate all of the resources provided by Infrastructure layer.

The third layer, on the top of the stack comprises of the applications or softwares which are required by operations groups.

As far as deployment models are concerned, we can divide Cloud in four types:

1. Public
2. Private
3. Vertical (community clouds)
4. Hybrid

[2] ISSUES AND CHALLENGES OF SECURITY IN THE CLOUD

The cloud service provides should understand the need to protect or secure customer's applications and data to be there in existing competitive environment. As per the opinions taken of 244 IT executives, security is on the top as far as issues and challenges are concerned in Cloud Computing [2].

Resources required to be protected in all three environments i.e. SaaS, PaaS, IaaS.

With cloud, the person will lose control over physical security of data. With public cloud, enterprise or person is sharing computing resources with other enterprises, where we don't know about the location or place where our resources are being accessed or shared.

Even with encryption, actually there is a question, who will control key management? Whether it is customer or service provider? The customer should be sure that he is managing the key for encryption.

Data integrity is another challenge where we require ensuring that data is identically managed during operations like transformation, retrieval etc.

Another key challenge in the cloud computing is data level security.

2.1 SAAS SECURITY

SaaS is dominating cloud service requirement now a day and will remain dominant in future also. This is the area where it is required to provide more sight on security aspects. The consulting firm Gartner has proposed seven security issues required to be discussed:

1. Privileged user access
2. Regulatory compliance
3. Data location
4. Data segregation
5. Recovery
6. Investigative support
7. Long term viability

Here is the checklist for SaaS [3]:

1. Is the security architecture documented in full?
2. Are special security aspects, such as application and platform security, taken into account, on which the security as a service functions are provided?
3. Do the cloud services have a security certificate?
4. How can the security functions be integrated as a service? Are there open interfaces and a user friendly portal?
5. Which cloud vendors and services are supported?
6. Where is security relevant data stored?

[3] SECURITY PRACTICES FOR SAAS ENVIRONMENT

The following practices should be followed for baseline security in SaaS environment [4].

1. Security Management and governance

One of the most important actions is to prepare complete agreement for security organization and program. This will introduce a vision in a team about what security leadership is driving towards and expects. The ownership will result in to a success of collective team. Clarity must be defined about roles and responsibility in agreement.

A steering committee should be planned with the objective to focus on providing guidance about security initiatives and its synchronization with business practices. The agreement for security team is the creation of steering committee.

Lack of proper management and governance results in potential security risks left unaddressed.

2. Risk management and assessment

Effective risk management requires identifying technological assets, data and its links to business process, applications and data stores and assignment of ownership and responsibilities. A proper risk assessment process should be created to allocate security resources linked with business continuity.

Risk assessment is important to help the organizational security decision making balanced between business utility and security of assets. Information security risk management process should measure security risks and plan and managing them periodically and when needed.

3. Security awareness and training

Human being is the weakest link of security. Improper awareness and training to needy people can expose company to number of security risks. Social engineering, slower responses to security incidents are possible risks. A tailored security awareness and training program is needed for individual based on his or her role and responsibility.

Programs that provide baseline for fundamentals of security and risk management skills and knowledge should be planned especially for security team and other internal personnel. Without adequate and current training, security team can not deal with problems.

4. Policies, standards and guidelines

Resources and templates are available to prepare information security policies, standards and guidelines. Security team should first of all identify information security and business requirements for cloud computing. Policies, standards and guidelines should be reviewed at regular interval.

5. Secure SDLC

Secure SDLC incorporates identification of threats and risks, followed by design and implementation aspects relevant to threats and risks.

The SecSDLC should provide consistency, repeatability and conformance. Here, the application code is written in a consistent manner which can be audited and enhanced. Core application services are provided in a common, structured and repeatable manner. Modules should be tested thoroughly for security issues. Internal and external penetration testing should be done to ensure security aspects of implementation.

6. Security architecture design

A security architecture design must be prepared by considering processes, operational procedures, organizational management, and security program compliance. SA document should be developed which defined security and privacy principles. The following services should be provided with security process:

a. Authentication
b. Availability
c. Authorization
d. Accountability
e. Integrity
f. Confidentiality
g. Privacy

The architectural design should be reviewed for new changes for better assessment.

7. Data privacy

A gap analysis of controls and procedures should be done. Based on these results, privacy procedures and initiatives should be defined and managed.

Based on size and scale of organization and operations, an individual person or team should be given responsibility for managing privacy. A team called privacy steering committee can be formulated to take decisions in privacy issues and problems.

8. Data governance

Data governance framework should be developed which defines a system for decision rights and accountability for processes related to information.

This data governance framework should include:

a. Classification
b. Analysis
c. Protection
d. Privacy
e. Inventory
f. Recovery / retention / discovery
g. Destruction

9. Data security

The data level security is the challenge in cloud computing environment. Sensitive data is domain of organization, not of service provider. Security should be there at data level so that organization can ensure data security wherever it goes.

10. Application security

This is one of the important factors for the success of any SaaS provider company. Here the security features and requirements are defined and application test results are reviewed. Collaborative efforts should be there between a security and development team for defining application security process, coding guidelines, training and testing tools and scripts.

External penetration testing can be done to identify loop holes of the system. This must be done at regular interval of time.

11. Identity Access Management (IAM)

Identity and access management are important functions for any organization. Expectation of SaaS customer is that least privileges should be granted to his/her data. Principle says that only minimum access should be granted to perform any operation and that is again for minimum time period.

Most of IAM solutions are designed to work in a controlled and static environment. User centric federated identity management solutions can be there.

In this dynamic cloud environment, models of trust assumptions, privacy and authentication and authorization implications are challenges. To meet these challenges new models can be developed suitable for SaaS providers.

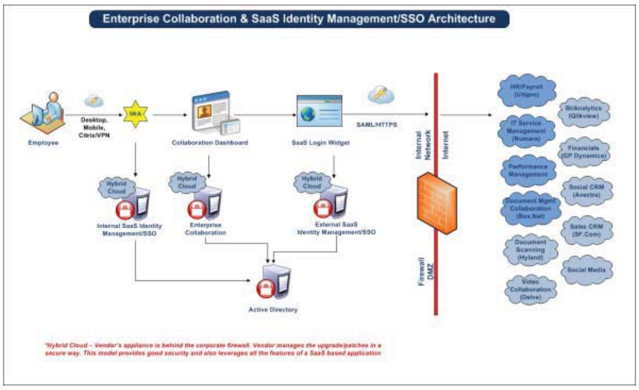
Enterprise Collaboration & SaaS Identity Management/SSO Architecture
Employee
Desktop, Mobile, Citrix/VPN
IWA
Collaboration Dashboard
SaaS Login Widget
SAML/HTTPS
Internal Network
Internet
Firewall DMZ
Hybrid Cloud
Internal SaaS Identity Management/SSO
Hybrid Cloud
Enterprise Collaboration
Hybrid Cloud
External SaaS Identity Management/SSO
Active Directory
HR/Payroll (Ultipro)
BI/Analytics (Qlikview)
IT Service Management (Numara)
Financials (GP Dynamics)
Performance Management
Social CRM (Avectra)
Document Mgmt Collaboration (Box.Net)
Sales CRM (SF.Com)
Document Scanning (Hyland)
Social Media
Video Collaboration (Delve)
*Hybrid Cloud – Vendor's appliance is behind the corporate firewall. Vendor manages the upgrade/patches in a secure way. This model provides good security and also leverages all the features of a SaaS based application

Fig. 1 -- Sample Identity Management Architecture for SaaS

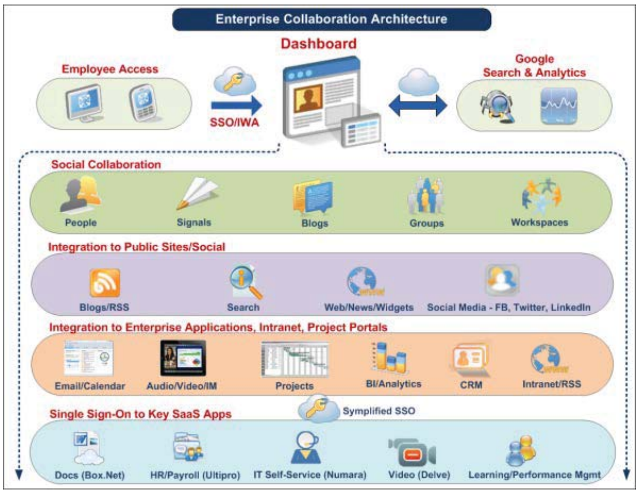

Fig. 2 -- Sample Enterprise Collaboration Architecture

[4] CONCLUSION

Here, we have seen security issues and challenges for SaaS. A security management team can be established which takes care of all aspects for policy, standard and their implementation as well as training and testing aspects which can be a part of SDLC. Similar kind of challenges can be there for IaaS and PaaS also.

REFERENCES

[1] Eric Marks, Bob Lozano, “Executive’s Guide to Cloud Computing”, John Wiley & Sons, 2010, pp. 28

[2] http://cloudsecurity.org/2008/10/14/biggest-cloud-challenge-security, retrieved 21 Feb. 2009.

[3] Werner Streitberger, Angelika Ruppel, “Cloud Computing Security Protection Goals, Taxonomy, Market Review”, Fraunhofer AISEC, 2010

[4] John Rittinghouse, James Ransome, “Cloud Computing – Implementation, Management and Security”, CRC Press, 2010

Biographies and Photographs

Mr, Divyakant Meva is working as Assistant Professor at FCA, MEFGI, Rajkot. He has an experience of 11.5 year. He has published more than 10 papers in International Journals. He is pursuing his Ph.D. From Saurashtra University.

Dr. C K Kumbharana is working as Associate Professor and Head at Department of Computer Science, Saurashtra University, Rajkot. He has more than 22 years teaching experience. His area of interest are speech processing and multimedia.