International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Security Measures on Mobile Technology Using Software as a Service (SaaS)

Apoorva P[1], Akshay S[2]

[1]Lecturer, Department of Computer Science, Amrita Vishwa Vidyapeetham, Mysore Campus, Karnataka, India

[2]Lecturer, Department of Computer Science, Amrita Vishwa Vidyapeetham, Mysore Campus, Karnataka, India

Abstract: ***Deploying cloud computing in an enterprise infrastructure brings significant security concerns. In this paper, we have discussed about security and concerns in cloud computing and enlightened steps that an enterprise can take to reduce security risks and protect their resources. This paper discusses the importance of security in Mobile Technology using Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Here all kind of authentication mechanism is used such as SAML based, SSO and LDAP based authentication for more security. For authorization XACML is used. By following OSGi standard security plug-in has been developed so that anybody can just add the plug-in as a jar file and get the security features such as LADP registration, authentication. So this system is more flexible and compact than others.***

Keywords: Iaas, SaaS, LADP, Cloud computing, Authentication.

1. Introduction

In a SaaS platform the security always play an important role. When a customer is going forward for a cloud platform there are “n” numbers of security issues present. Each and every user of SaaS platform should be identified separately, authenticated and authorized. A user should authenticate via LDAP (Directory Server) in a cloud platform for more flexible use and authorized to get the resource based on his/her role defined by the administrator. The authentication can be done through SAML (Security Assertion Markup Language) and authorization through XACML (Extensible Access Control Markup language). The security solution should follow the OSGi framework. It should follow the WS Security to provide message level security. This is to identify each and every user in a cloud platform. This is responsible to authenticate and authorize a user, provide role-based access for a user, create policies and rules for controlling access information. And also provide security for multitenant environment and ensure WS Security. This solution supports OSGi so any client who wants to get a security solution they can get it as a plug-in to their SaaS solution. And also it supports on premise as well as an instance so that anybody can use it because it also supports security as a service. Because of the massive popularity of android, the users who is using the android phone they can get access to their work environment securely by using this solution. So this is another advantage of this. It supports android also.

Cloud computing providers offer their services according to three fundamental models. Infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS) where IaaS is the most basic and each higher model abstracts from the details of the lower models. This provides the Application level security for SaaS platform. In SaaS platform the main advantage is it supports multitenant architecture. In a SaaS model, the organization is a tenant, not an owner, but the groups of employees are still users. Each user has an association to a particular tenant (organization) and SaaS provides each tenant with the experience of owning their own copy of the application, which their users can use. It needs to provide a mechanism to support user identification and authentication that allows for the unique identification of users. Because multi-tenancy requires that all the users that sign-on to the system be identified to determine which tenant they belong to, there has to be a definitive relationship that allows for users to be identified as belonging to a particular tenant. That user-to-tenant relationship is the key information that is used to restrict the data that can be accessed by the user. Email addresses are a typical way of doing this so that uniqueness is assured and individuals can be recognized and identified as belonging to a particular tenant. There are many authentication mechanisms and methods of integration with them, so a flexible mechanism for allowing a user to be identified is essential. It is often necessary that a particular tenant be able to utilize their existing LDAP or other directory service or authentication mechanism to support SAML based single sign-on to the SaaS application. Although this type of external authentication of the user is important, it's the responsibility of the SaaS application to establish that the identified user is a member of the tenant they claim.

2. System function

2.1 Product Function:

It will provide security for SaaS platform. SaaS supports multitenant architecture. In this scenario security is very useful. Security for authentication, authorization, and it should take care that nobody else gets access to other resources as well as others platform which is not belong to them. So there will be site to site VPN for confidentiality. Provide security for APIs also. It also makes sure that right people should get the right access information. From Figure 1 we can see that the user may send request from any kind of terminal. From user the request will go through http/https hyper text transfer protocol or secure hyper text transfer protocol which will be reached to the de militarized zone through firewall if the user is authenticated and then it will go to the web server then user verification and access checking will be done. Then web server communicates to the application server through IIOP/ORB (Internet Inter-ORB Protocol). Then the request will be sent to another firewall level security which will later reach to the application server. Before this there will be a checking based on rules and policies specific to the user. These policies will be written along with SOAP through SAML. XACML will provide the authorization request. For authentication directory server plays a big role. All user credentials stores inside the directory server and it maintains a tree structure. So fetching credentials will be very easy and this credential will help to authenticate a user.

2.2 Module Description:

The entire work can be divided into following modules:

1. Authentication through LDAP

LDAP is a directory server and here we are using Apache DS. Inside this all the credentials will store as a tree structure for easy access. A user will authenticate through the LDAP based on the company rules and what kind of credential they want to use for a security solution. So here we are assuming LDAP as an actor and the credentials are use cases. Another actor user will authenticate through LDAP. This authentication can be done as on premise as well as LDAP security as a web service.

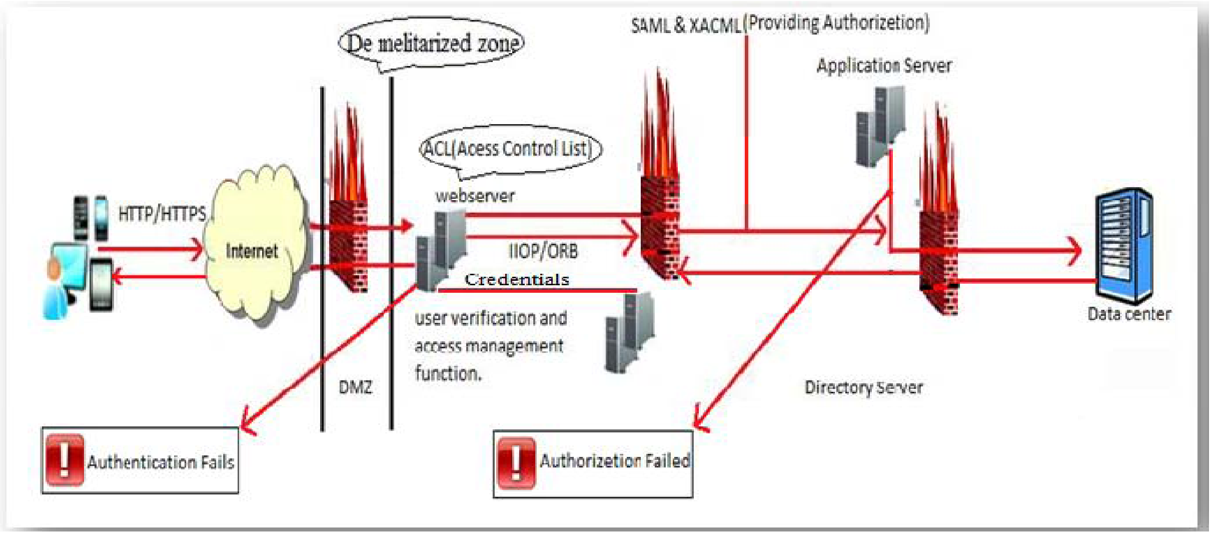

Figure 1: Secure SaaS platform

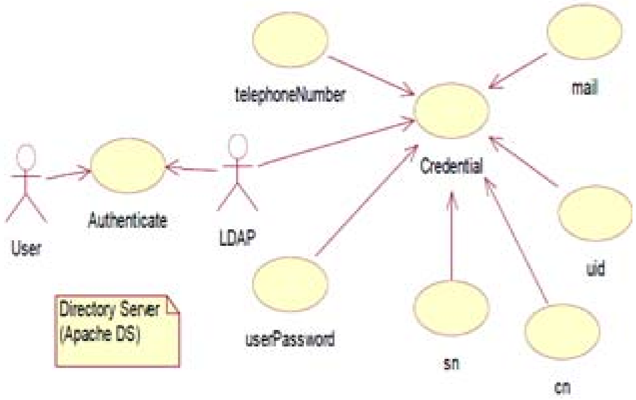

Figure 2: Authentications through LDAP

2. Authentication through SAML

SAML-SSO (SAML Single Sign On) is having following divisions i) Relying party, ii) Attribute Assertion, iii) IdP (Identity Provider). It authenticates a user. Here we used WSO2 identity server as a identity provider. WSO2 is an open source server and it supports cloud platform as well as on premise. So the resource needs to be uploaded inside the SAML SSO page inside identity server. Then whenever the resource is called the user should authentication through SAML before getting in the resource. Here SAML API used. From Figure 3 we can see that the use of SAML-SSO (SAML Single Sign On).

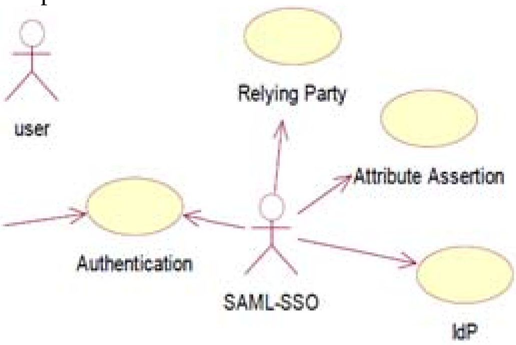

Figure 3: *Authentications through SAML*

3. Authorization through XACML

XACML is responsible for authorization and it is having 4 parts, such as

i) PDP
ii) PEP
iii) PAP
iv) PIP

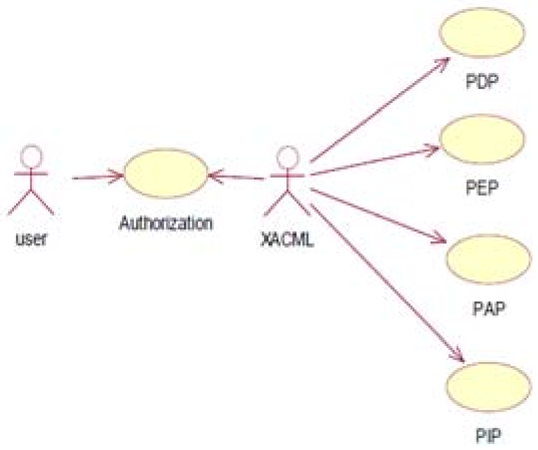

Figure 4: Authorizations through XACML

Here also we used WSO2 identity server to upload a XACML policy based on the user roles. Let assume that there will be a sample policy by which a group of user will authorize to get inside a resource based on their designation and they are only having the read permission. This all roles are policy can be customizable based on the requirement. That resource can be anything any web services which is available for the user but only after proper authorization. The diagram of the authorization is shown in Figure 5.

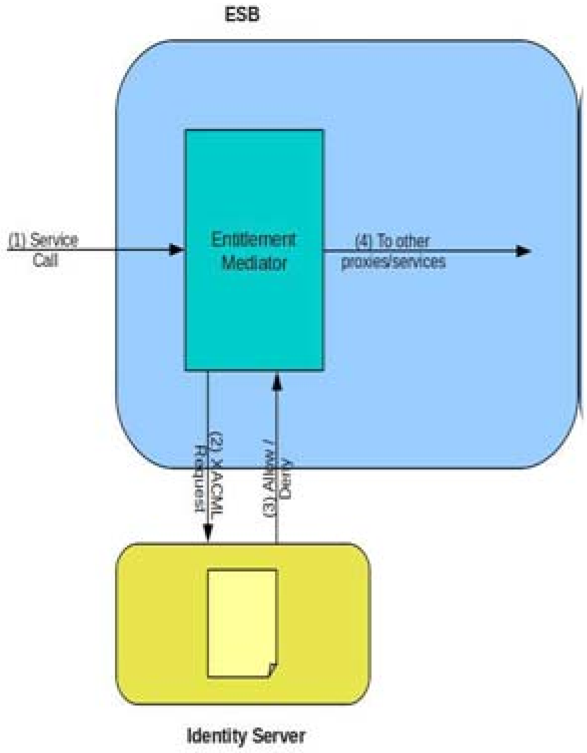

Figure 5: Authorization

4. Security plug-in follows OSGi framework

This security solution follows OSGi standard. So there is no interoperability issue will come. Because it is a plug in so anybody who wants to secure their platform they need to just install this plug in. no need to build a security solution again. So from business point of view it is a proper cost cut. And also OSGi is an emerging framework now most of the industry follows this to build their product.

5. WS-Security

Through this we can ensure the application security by writing a web service and securing it by providing username and password.

So the outcome of this solution is providing secure platform for SaaS based application. As well as to ensure right people should get right access. User should get his/her resources and API's based on the predefined rules and policies. Because it is a multitenant system so make sure that no two working environment should coincide with each other. User should get the server based on the configuration. Write roles, policies and access control list based on the requirement. Secure the platform from other network attack. So it is an encapsulate security solution for SaaS environment. There will be a web service client where we need to put the user name and password inside the request header. On the **web service server** site, get the request header parameters via WebServiceContext. So the client sends the request with username and password is included inside the SOAP envelop and the server sends back the normal response. So finally we are writing the web service to authenticate a user and based on the authentication he/she will get some kind of resource or access.

3. Conclusion

Through this paper, we tried to design a product which supports multitenant architecture and also which is based on OSGi frame work. It is easy to use and it is flexible and platform independent because it is developed as an instance so it is available to all platform. We used two type authentication methods those are LDAP and SAML. For authorization XACML is used. Which provides more security and ensure that a user in a multitenant environment should authenticate and authorize based on credentials, assertion attributes and policies respectively.

4. Future Work

Cloud computing data can be represented in different ways to make the above discussed method work efficiently. Various softwares related to security can be designed to improve the level of security given to cloud data. This software can be designed to be a SaaS for better security.

References

[1] Anthony Bisong and Syed (Shawon) M. Rahman,'An overview of the security concerns in enterprise cloud computing', International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.1, January 2011.

[2] Armbrust, M. Fox, A, Griffith, R. Joseph, D. A. Katz, R. Konwinski, A. et al. (2009, February). Above the clouds: A Berkeley View of cloud computing. Retrieved on March 10,2010 from
Available:
http://d1smfj0g31qzek.cloudfront.net/abovetheclouds.pdf.

[3] Stubblefield, A; et al. (2004) 'A Key Recovery Attack on the 802.11b Wired Equivalent Privacy Protocol

(WEP)' in ACM Transactions on Information and System Security, Vol. 7, No. 2, May 2004, pg 319–332.

[4] Ijeh, A.C., Preston, D.S., Imafidon, C.O. (2009) "Security Strategy Models (SSM)" In the Proceedings of the 4th Annual' Advances in Computing Technology Conference (AC&T). 27 January 2009 pp.126-131 University of East London United Kingdom
Available: http://www.uel.ac.uk/act/index.htm

[5] Mahajan, R. (2006) 'Analyzing the MAC-level Behaviour of Wireless Networks in the Wild' in ACM SIGCOMM Computer Communication Review , Proceedings of the 2006 conference on Applications, technologies, architectures, and protocols for computer communications SIGCOMM '06, 36(4) pg75.

[6] Gruteser, M. and Grunwald, D. (2005) 'Enhancing Location Privacy in Wireless LAN through Disposable Interface Identifiers: a Quantitative Analysis' Mobile Networks and Applications, 10(3) pg 315-325

[7] Kowitz, B. and Cranor, L. (2005) 'Peripheral Privacy Notifications for Wireless Networks' in Proceedings of the 2005 ACM workshop on Privacy in the electronic society WPES '05. pg 90-96

[8] Juha K. Laurila , Daniel Gatica-Perez, Imad Aad, ' The Mobile Data Challenge: Big Data for Mobile Computing Research'.

[9] http://www.wso2.org/library/articles.

[10] http://www.vogella.com/articles/OSGi.

Author Profile

Apoorva P received M.Sc. degree in Computer Science from University of Mysore in 2011. From 2011 she is working as a lecturer in Department of Computer Science, Amrita Vishwa Vidyapeetham, Mysore Campus. Her areas of interests are Pattern Recognition, Digital Signal Processing, Computer networks and network security.

Akshay S received M.S. degree in Computer Science from University of Mysore in 2012. From 2012 he is working as a lecturer in Department of Computer Science, Amrita Vishwa Vidyapeetham, Mysore Campus. His areas of interests are Pattern Recognition, Digital Signal Processing, Image Processing, Algorithms and Data structures.