Shalu Soni al. International Journal of Recent Research Aspects ISSN: 2349-7688, Vol. 1, Issue 2, Sept. 2014, pp. 18-21

Analyzing the Cloud Computing security issues with JAAS Module

Shalu Soni[1], Sahil Verma[2], Kamal Kumar Sharma[3]

[1]Student, M. Tech, ESEAR, Ambala

[2]Assistant Professor, Dept. of CSE, E-Max group of Institutions, Ambala

[3]Professor, Dept. of ECE, E-Max group of Institutions, Ambala

Abstract. **The significance of Cloud Computing is growing and it is receiving a growing attention in the scientific and industrial communities. Security concerns relate to risk areas such as external data storage, dependency on the "public" internet, lack of control, multi-tenancy and integration with internal security. Compared to traditional technologies, the cloud has many features, such as its large scale and the resources belonging to cloud providers are completely distributed, heterogeneous and totally virtualized. Traditional security mechanisms such as identity, authentication, and authorization are no longer enough for clouds in their current form .In this paper,we have discussed the security issues of cloud computing and also provided the existing solution for implementing cloud computing security. An overview of Java Authentication and Authorization Service, or JAAS, i.e. Java implementation of the standard Pluggable Authentication Module (PAM) information security framework is given in this paper.**

Keywords— **Cloud computing, JAAS, SAAS, PAAS, IAAS**

I. INTRODUCTION

Cloud computing is a collection of IT services that are provided to a customer on a leased basis over a network and with the ability to scale up or down their service requirements. Usually cloud computing services by a third party source are delievered who owns the infrastructure. It advantages to mention but a small number of include scalability, resilience, flexibility, efficiency and outsourcing non-core activities. Cloud computing offers an modern business model for organizations to accept IT services without open investment. The organizations are slow in accepting it due to security issues and challenges associated with it, despite the potential gains achieved from cloud computing.

There are numerous cloud computing providers including Google, Salesforce, Yahoo, Microsoft, Amazon, and others that are providing cloud computing services (Figure1. shows current cloud providers).Cloud computing providers provide a series of services include e-mails, storage, software-as-a-services, infrastructure-as-a-services etc to the customers.

Software as a Service(SAAS)

Software as a Service is the most fundamental form of cloud computing. There is no third-party expansion or resources for the user, but SaaS applications can present powerful tools right from your web browser. Example of SaaS is Google Docs. Google Docs is a productivity suite that is free for anyone to use. Creating a Google account is free. All you have to do is log in to google.com/docs and you immediately have right to use to a powerful word processor, spreadsheet application, and presentation creator. These online services provided by Google are managed directly from the web browser and require zero installation. You can access your Google Docs from any computer or mobile device with a webbrowser.GoogleDocs, Dropbox, Box.net, Salesforce.com and Freshbooks are all applications that qualify as SaaS. All of these applications are either free to use, or offer more features at a paid subscription price. Another advantage of SaaS applications is the ability to work together with others cheaply and from any location.

Platform as a Service(PAAS)

Platform as a Service is the second segment of cloud services, provides developers with proprietary APIs to make an application that will run in a particular environment. While a developer is free to create any application they wish, the app is locked to the platform used for its creation. This method of developing applications can be at low cost (through some providers, even free) and allows you to influence the infrastructure and tools of an already established cloud company for building or migrating your existing applications. This also gives you the ability to quickly make your app available to a wide audience.

The simpler example of PaaS is Facebook. Developers can create particular applications for the Facebook platform using proprietary APIs and make that app available to any Facebook user. Some applications combine a user's Twitter and Facebook account, others integrate a database with a Facebook profile. The downside to PaaS is whatever platform you choose to develop in, you can only use the tools and languages they provide. Plus the granularity of operation may be limited to what the API exposes; you may not get machine-level control and flexibility.

Infrastructure as a Service(IAAS)

The third division of cloud services is known as IaaS, or Infrastructure as a Service. This is the most comprehensive cloud platform and is mainly used by large-scale enterprise customers or full-time developers. SaaS allows usage of cloud apps, and PaaS allows you to develop apps, IaaS gives you infrastructure for developing, running, and storing your apps in cloud environments. The advantage

of IaaS is the virtually unlimited storage and computing power available to developers without having any physical hardware on site.

Amazon EC2 is good example of IaaS. From the smallest application to full-scale websites, EC2 provides commodity cloud infrastructure to run them all.

The diagram below depicts the Cloud Computing stack – it shows three different categories within Cloud Computing: Software as a Service, Platform as a Service and Infrastructure as a Service.

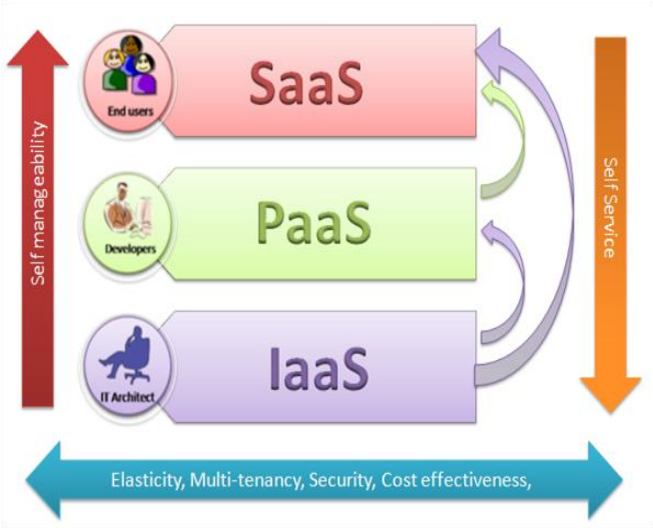

Figure 1

I. SECURITY ISSUES IN CLOUD COMPUTING

The significance of Cloud Computing is growing and it is receiving a growing attention in the scientific and industrial communities. Cloud Computing as the first among the top 10 most important technologies and with a better prospect in successive years by companies and organizations.

Cloud Computing enables convenient, ubiquitous, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be quickly provisioned and released with minimal management effort or service provider interaction.

Security concerns relate to risk areas such as external data storage, dependency on the "public" internet, lack of control, multi-tenancy and integration with internal security. Compared to traditional technologies, the cloud has many features, such as its large scale and the resources belonging to cloud providers are completely distributed, heterogeneous and totally virtualized. Traditional security mechanisms such as identity, authentication, and authorization are no longer enough for clouds in their current form [11]. Security controls in Cloud Computing are no different than security controls in any IT environment. However, because of the cloud service models employed, the operational models, and the technologies used to enable cloud services, Cloud Computing may present different risks to an organization than traditional IT solutions. Unfortunately, integrating security into these solutions is often perceived as making them more rigid. There are various 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. Therefore, security issues for many of these systems and technologies are applicable to cloud computing. For example, the network that interconnects the systems in a cloud has to be secure. Fur. In addition, resource allocation and memory management algorithms have to be secure. Finally, data mining techniques may be applicable to malware detection in clouds.

The Cloud Security Alliance (Cloud Computing Alliance, 2010) did a research on the threats facing cloud computing and it identified the *flowing major threats:*

- Failures in Provider Security
- Attacks by Other Customers
- Availability and Reliability Issues
- Legal and Regulatory Issues
- Perimeter Security Model Broken
- Integrating Provider and Customer Security Systems
- Insecure Application Programming Interfaces
- Malicious Insiders
- Shared Technology Vulnerabilities
- Data Loss/Leakage
- Account, Service & Traffic Hijacking
- Unknown Risk Profile

II. EXISTING SOLUTION FOR IMPLEMENTING CLOUD SECURITY

Kuyoro et. al (2011) introduced a detailed analysis of the cloud computing security issues and challenges focusing on the cloud computing types and the service delivery types. Inspite of the potential gains achieved from the cloud computing, the organizations are slow in accepting it due to security issues and challenges associated with it. Security is one of the major issues which slow down the growth of cloud. The idea of handing over significant data to another company is worrisome; such that the consumers need to be vigilant in understanding the risks of data breaches in this new environment.

Hamlen et. al (2011) discussed security issues for cloud computing and present a layered structure for secure clouds which focus on two of the layers, i.e., the storage layer and the data layer. In particular, the authors discuss a scheme for secure third party publications of documents in a cloud. Next, the paper will converse secure federated query processing with map Reduce and Hadoop, and discuss the use of secure co-processors for cloud computing. Finally, the authors discuss XACML implementation for Hadoop and discuss their beliefs that building trusted applications from untrusted components will be a major aspect of secure cloud computing.

Zhao et. al (2011) introduced completely homomorphism encryption algorithm in the cloud computing data security. This new security solution is fully fit for the processing and retrieval of the encrypted data and effectively leading to the broad applicable prospect， the security of data transmission and the storage of the cloud computing.

Gonzalez et. al (2011) migrating to the cloud remains a attractive trend from a financial perspective, there are several other aspects that must be taken into account by companies before they decide to do so. One of the most important aspect refers to security: while some cloud computing security issues are inherited from the solutions adopted to create such services, many new security questions that are particular to these solutions also arise, including those related to how the services are organized and which kind of service/data can be placed in the cloud. Aiming to give a better understanding of this complex scenario, in this article we identify and classify the main security concerns and solutions in cloud computing, and propose a taxonomy of security in cloud computing, giving an overview of the current status of security in this emerging technology.

Min et. al (2012) tried to study the threats and attacks that possibly launch in cloud computing and the possible solutions to mitigate these attacks. Aside of having network and application securities being adopted, there must be a security that authenticate the user when accessing the cloud services that is bound to the rules between the cloud computing provider and the client side.

Khalil et. al (2014) provide a comprehensive study of cloud computing security and privacy concerns. We identify cloud vulnerabilities, classify known security threats and attacks, and present the state-of-the-art practices to control the vulnerabilities, neutralize the threats, and calibrate the attacks. Additionally, we investigate and identify the limitations of the current solutions and provide insights of the future security perspectives.

Finally, we provide a cloud security framework in which we present the various lines of defense and identify the dependency levels among them. We identify 28 cloud security threats which we classify into five categories. We also present nine general cloud attacks along with various attack incidents, and provide effectiveness analysis of the proposed countermeasures.

AL-SAIYD designed a cloud computing security development lifecycle model to achieve safety and enable the user to take advantage of this technology as much as possible of security and face the risks that may be exposed to data. A data integrity checking algorithm; which eliminates the third party auditing, is explained to protect static and dynamic data from unauthorized observation, modification, or interference.

III. JAAS

Java Authentication and Authorization Service, or **JAAS**, pronounced "Jazz", is the Java implementation of the standard Pluggable Authentication Module (PAM) information security framework. JAAS was introduced as an extension library to the Java Platform, Standard Edition 1.3 and was integrated in version 1.4.

The main goal of JAAS is to separate the concerns of user authentication so that they may be managed independently. While the former authentication mechanism contained information about where the code originated from and who signed that code, JAAS adds a marker about who runs the code. By extending the verification vectors JAAS extends the security architecture for Java applications that require authentication and authorization modules.

Administration

For the system administrator, JAAS consists of two kinds of configuration file:

- ***.login.conf**: specifies how to plug vendor-supplied login modules into particular applications
- ***.policy**: specifies which identities (users or programs) are granted which permissions

Application Interface

For the application developer, JAAS is a standard library that provides:

- a representation of identity (Principal) and a set of credentials (Subject)
- a login service that will invoke your application callbacks to ask the user things like username and password. It returns a new *Subject*
- a service that tests if a Subject was granted a permission by an administrator.

Security System Integration

For the security system integrator, JAAS provides interfaces:

- to provide your identity namespace to applications
- to attach credentials to threads (*Subject*)
- for developing login modules. Your module invokes callbacks to query the user, checks their response and generates a *Subject*.

Login Modules

Login modules are primarily concerned with authentication rather than authorization and form a widely used component of JAAS. A login module is required to implement the javax.security.auth.spi.LoginModule interface, which specifies the following methods:

Note: A Subject is the user that is attempting to log in.

- initialize: Code to initialize the login module, usually by storing the parameters passed into appropriate fields of the Class.
- login: Actually check the credentials provided via an Object that implements the javax.security.auth.Callback interface (e.g. check against a database). This method could prompt the user for their login and password or it could use details previously obtained. It is important to note here that, if invalid credentials are supplied then a javax.security.auth.login.FailedLoginException should be thrown (rather than returning false, which indicates that this login module should be ignored, which potentially allows authentication to succeed).
- commit: The identity of the subject has been verified, so code in this method sets up the Principal and Groups (roles) for the successfully authenticated subject. This method has to be written carefully in enterprise applications as Java EE application servers often expect the relationships between the Principal and Group objects to be set up in a certain way.This method should throw a javax.security.auth.login.FailedLoginException if authentication fails (e.g. a user has specified an incorrect login or password).
- abort: Called if the authentication process itself fails. If this method returns false, then this Login Module is ignored.

- logout: Code that should be executed upon logout (e.g. could remove the Principal from the Subject or could invalidate a web session).

Login modules can provide single sign on (SSO) via a particular SSO protocol/framework (e.g. SAML, OpenID, and SPNEGO), can check for the presence of hardware security tokens (e.g. USB token), e.t.c. In an n-tier application, Login Modules can be present on both the client side and server side.

LoginModule (javax.security.auth.spi.LoginModule)

Login modules are written by implementing this interface; they contain the actual code for authentication. It can use various mechanisms to authenticate user credentials. The code could retrieve a password from a database and compare it to the password supplied to the module.

LoginContext (javax.security.auth.login.LoginContext)

The login context is the core of the JAAS framework which kicks off the authentication process by creating a Subject. As the authentication process proceeds, the subject is populated with various principals and credentials for further processing.

Subject (javax.security.auth.Subject)

A subject represents a single user, entity or system –in other words, a client– requesting authentication.

Principal (java.security.Principal)

A principal represents the face of a subject. It encapsulates features or properties of a subject. A subject can contain multiple principals.

Credentials

Credentials are nothing but pieces of information regarding the subject in consideration. They might be account numbers, passwords, certificates etc. As the credential represents some important information, the further interfaces might be useful for creating a proper and secure credential javax.security.auth.Destroyable&javax.security.auth.Refresh able. Suppose that after the successful authentication of the user you populate the subject with a secret ID (in the form of a credential) with which the subject can execute some critical services, but the credential should be removed after a specific time. In that case, one might want to implement the Destroyable interface. Refreshable might be useful if a credential has only a limited timespan in which it is valid.

IV. FORM AUTHENTICATION

Form authentication is another commonly used part of JAAS. In this process the user is typically presented with a web page containing a form asking for a username and password. This data is then submitted via POST to a URL containing the text "j_security_check", e.g. www.example.com/j_security_check . The credentials are checked on the server side and a session ID is returned to the client via a cookie. This authentication method is flexible in that a Java HTTP client such as Apache HTTP client can be used in place of a web-browser, e.g. in a desktop application, as long as the following standard steps are followed:

- Request a protected URL (i.e. secured via a security-constraint element) in web.xml (where the login-config element has specified an authentication method of "FORM").
- The server will return a redirect (302) to the security check URL mentioned above along with a cookie containing the session ID ("JSESSIONID=...").
- Send the username and password (encoded as form fields) along with the cookie via an HTTP POST to the security check URL.
- If authentication is successful, the server will send a 302 back to the original protected URL.
- Send a GET request to that URL, passing the session ID cookie (preferably assert that the response contains what you would expect from that original URL).

V. CONCLUSION

Traditional Security mechanisms such as identity, authentication, and authorization are no longer enough for clouds in their current form .The security issues of cloud computing are studied and the existing solution for implementing cloud computing security are discussed. The cloud computing issues are analyzed along with JAAS (Java Authentication and Authorization Service)modules are analyzed in this paper.

REFERENCES

[1]. Kuyoro S. O., Ibikunle F. & Awodele O., "Cloud Computing Security Issues and Challenges", International Journal of Computer Networks (IJCN), Volume (3) : Issue (5) : 2011, pp. 247-255.

[2]. Kevin Hamlen, Murat Kantarcioglu, "Security Issues for Cloud Computing", International Journal of Information Security and Privacy, 4(2), 39-51, April-June 2010 .

[3]. Issa M. Khalil 1,*, Abdallah Khreishah 2 and Muhammad Azeem 3, Cloud Computing Security: A Survey, *Computers* 2014, *3*, 1-35.

[4]. Theodore J. Shrader, Bruce A. Rich Anthony J. Nadalin. JavaTM and internet security. p. 152.

