



RESEARCH ARTICLE

SECURING CLOUD COMPUTING ENVIRONMENT USING TIME DELAY BASED ON SESSION

Koteswar rao.M¹, Mr. G. Sree Ram²

¹M-Tech, Computer Science and Engineering, Dr. MGR Educational and Research Institute University,
Chennai-6000095, India

²Assistant Professor, Computer Science and Engineering, Dr. MGR Educational and Research Institute
University, Chennai-6000095, India

Corresponding Author Email: ¹mandlakoteswar2011@gmail.com

Abstract— Cloud Computing is an emerging technology in today's computers world. It has various benefits such as resource sharing, reliability and highly accessible. There is a main drawback of cloud computing is security to threats from attackers. In cloud computing where infrastructure is shared millions of users. So responsibility of cloud service provider (csp) is to provide the security to the data from attackers. In this paper, it is proposed to secure the cloud computing data using time delay.

Key Terms: - cloud computing; data security; cloud security; session tracking; time delay

I. INTRODUCTION

Cloud Computing faces new challenging security threats for number of reasons. Security Issues in Cloud Computing is [1] Browser Security, XML Signature Element Wrapping, hosting malicious data, Cloud Malware Injection Attack and Flooding Attacks. The cloud service provider provides authentication and some security to its services although it will also have threats, there is a need to protect the data in the cloud.

The cloud service provider (csp) has provided security and authentication methods to the information. Sometimes user also makes the mistakes for registering data and accessing data in cloud computing. To overcome this issue the cloud service provider fixes the time interval in the cloud.

In this paper, the data security for the cloud is implemented using the cloud foundry [2].cloud foundry is an open platforms a service (paas), providing a developer frame works and application services. Cloud Foundry makes it fast and easy to build, test, develop and scale applications.

In session management [3] client first make a request for any servlet or any web page. The container receives the request and generates a new unique session ID and get back to the client along with the response.

Outline of this paper:

The remainder of this paper is organized as follows. Section 2 introduces the basics and features of Cloud Foundry, Session Based Tracking. Section 3 elaborates on the process of Session Blocking user. Section 4 summarizes the paper.

II. BASICS AND FEATURES

2.1 Cloud Foundry

Cloud Foundry is an open platform as service developed by VMware started in 2011. Choice of clouds for development, across public, private and hybrid clouds, including Cloud Foundry. Cloud Foundry let the developers focus on writing the applications and the not meddling with middleware and infrastructure services.

Features:

1. No Vendor Lock in

PaaS in users can avoid vendor lock with specific PaaS vendors by using the open source Cloud Foundry. In generally, PaaS offers different usage such the API that is provided or the process used to develop applications. This means that is difficult to migrate the application developed for a specific PaaS to another.

2. Flexible Configuration

Cloud Foundry is design with flexibility to satisfy a huge variety of needs for PaaS environment. Cloud Foundry support the wide range of environment from a private PaaS on a single server to a huge public PaaS on a cluster of over a thousand servers and can be set up to suit the scale as well as its reliability and support features.

3. Support for languages and frameworks

Cloud Foundry supports most of the programming languages such as python, Java, and Java Script. It supports the different of famous frameworks used for building web applications. For example Spring, Sinatra, Ruby on rails is support to as default. PostgreSQL, MySQL, and also supported DBMS.

2.2 Session Base Tracking

For session tracking [5], is both internal and external session IDs are supported. The External session IDs are provided by the server, and delivered the user request. The user ID is generated by a session manager deliver to the as part of the publish URL. The client downloads the file at the start the content. Thecookies is sent to all subsequent and video fragment requests. If a user session ID is not received, then internal session ID is internal purposes.

The session of activity a user with a unique IP address spends the Web site during a specified period of time. The number of user sessions on a web site is used in measuring the amount of traffic and get web site. The site administrator determines what the time frame of a user session will be (e.g., 60 seconds). If the visitor comes back to the site within that time period, it still consider one user session because any number of visits within that 30 minutes will only count as 1 session. If the visitor returns to the web site after the allotted time period is expired, say an hour from the initial visit, then it's counted as a separate user session.

Algorithm:

Step 1: Session created for each user

Each user can created session for entering the web services.

Step 2: Activities Track

With number of activities is greater than genuine user activity then is blocked or otherwise allowed.

Step 3: Time track

Once will block the user id after some particular time allow the user id.

Pseudo code:

Set the session is created to each user

While number of activities is greater than genuine user activity

Session is blocked

Else

Session is allowed

Allow the user a specified period of time.

2.3 Cloud Foundry App Engine

Cloud Foundry allows user to run web applications on cloud infrastructure. Cloud foundry applications are easy to build, maintain, and scale as user traffic and data storage increases. The service can be run on private cloud or public cloud, built behind the firewalls. They must design to work with the broad range of programming languages and other cloud services are includes building on VMware.

Users can develop their application for the Java runtime environment using common Java web development tools and API standards. The platform currently supports Ruby on Rails, Java, Node.js, and Sinatra Ruby framework.

General opinion about to implement PaaS cloud particular Azure and App Engine is this drawback is requirement to be developer work inside a particular environment. App Engine built the use to Python, but has expand the include Java. Azure is a primarily focused on Microsoft's .NET framework the company is reported to working on the modules support PHP, Python, and Ruby others.

The Cloud Foundry design and goal, suggested by VMware, the broad to enough support the make it possible to developer to move their applications Cloud Foundry to environments from other PaaS cloud.

III. IMPLEMENTATION

In this paper the block the IP address and set the particular time for accessing the data. Sometimes genuine user also makes the mistakes for accessing the data. That time the user may access the data after particular some time. To access the Cloud foundry the user needs to create an account [4] in it to provide the necessary details and billing information. This will provide the user to select specific resources and pay as they use.

The cloud foundry can be accessed by using web browser or by using Eclipse API which allows the user to create their programs that can be executed on the cloud. The programming languages support by it is JAVA, VB, RUBY, PYTHON and PHP.

The Eclipse API should be first configured with the Google by installing the plug-in which will gives the user to interact and access data with the cloud.

Procedure:

Step 1: Create a Cloud Foundry account.

Step 2: Request for necessary resources that is required and select the resource usage amount.

Step 3: Create database with the necessary tables.

Step 4: Configure the Cloud Foundry API to access the services in the cloud.

Step 5: Develop a Cloud the virtually in micro Cloud Foundry.

Step 6: Create code for the Session Based Tracking algorithm in java.

Step 7: Create an AppEngine application to execute the code in cloud.

Step 8: Session tracking the using execute code in cloud.

Step 9: Not permitted to access the particular time.

Step 10: Allow accessing the web pages after some particular time.

IV. CONCLUSION

In this paper the Session Based Tracking algorithm has been implemented to access data in the Cloud Foundry. This will provide a session block the user up to some particular time. The user can get additional security up to some particular time. However security is in fact to be implemented alongside functionality and performance.

To find the source of real attackers, and block the attacker IP address. Able to detect the most of the attacker messages with in a very short period of time.

REFERENCES

- [1] Trostle J, (2006), "protecting Against Distributed Denial of service attacks Using Distributed Filtering," Securecomm and Workshops, Aug 28 2006- sept1 2006, pp 1-11
- [2] <https://developers.google.com/cloudfoundry/>
- [3] <http://pdf.coreservlets.com/Session-Tracking.pdf>
- [4] <https://my.cloudfoundry.com/signup>
- [5] [http://en.wikipedia.org/wiki/Session_\(computer_science\)](http://en.wikipedia.org/wiki/Session_(computer_science))

Authors Profile

Author M. Koteswar Rao M.Tech, student in Computer Science and Engineering, Dr. MGR Educational & Research Institute, Chennai, Tamilnadu, India.

E-mail – Mandlakoteswar2011@gmail.com