

Library Management System Implementation on Google App Engine(GAE) Cloud Infrastructure

Soe Yan Naung, Dr. Sabai Phyu

University of Computer Studies, Yangon, Myanmar

synappengine@gmail.com, sabaiphyu72@gmail.com

Abstract

All of the library systems need their own data centers for managing large data storage. Traditional library management needs more control over the management applications and stored data contains sensitive and private information. Web-based digital library provisioning and maintenance of infrastructure presents several challenges. Cloud computing is particularly attractive choice for library management system because of its large storage volume and streamline of cost. The proposed system will present the access control on library management system of university in cloud computing by utilizing the platform as a service(PaaS) of cloud. In this system, Google App Engine(GAE) will be used for the library management development. As the cloud service provider uses the multi-tenancy model, the data in the cloud is accessible to multiple users. Thus, there is a high risk to the security of data in the cloud. Therefore, there is a great need for providing security against these un-trusted service providers. So, this system also supports the data access control by Mandatory Access Control(MAC).

Keywords: PaaS, GAE, MAC, access control.

1. Introduction

As emerging in technology, cloud computing is rapidly used by many companies because of a lot of benefits can provide by cloud (for instance: cloud computing can support large storage space but the development cost is low and can also support virtualization and resource sharing). So, users can store enormous amount of data in cloud and the data stored in cloud can access from anywhere, anytime. In the cloud, shared data and stored resources need to provide access to only authorized user. This access permission can be control by the access control mechanisms which grant the authorized users to access the data and blocked the access from unauthorized

users. Each of these mechanisms has its own security controls to ensure the security and privacy of user's data.

2. Related Works

“The Efficient Multi-Tiered Storage System on Private Cloud”, Cho Cho Khaing [2010]: Data grew for IT managers, and they looked for every opportunity to improve their storage utilization and efficiency. This proposed system reduced hardware costs and management overhead. Multi-Tiered Storage System controlled and managed the different types of service levels as well. By using de-duplication, process saved space, improved data protection and increased speed. Reducing the amount of data redundancy made backups more efficient and quicker as well. Thus, Network bandwidth improved after de-duplication.

“Implementation of Multi-Level Security System Based on Mandatory Access Control(MAC) Using Roles”, Thwe Thwe Win Tun [2011]: Data is very important and necessary for performing and managing system's information resources. Security mechanisms are required to build critical software systems to obtain the reliability, integrity and availability. Now, modern database management system supports discretionary access control(DAC) and mandatory access control(MAC). In mandatory access control(MAC), each data is labeled with a certain classification level and each user is given a certain clearance level. Database management system that supports mandatory controls are also called multi-level secure system(MLS). The proposed system presented the implementation of health care information management security system using MAC with the combination of user's roles by labeling with clearances and all patient's data are classified. Four levels of classifications are top secret, secret, confidential and unclassified will be utilized to implement the necessary controls for the system.

3. Background Theory

Nowadays, cloud computing is becoming the major advancements to the IT industry. Grid and utility computing are new evolutionary models of cloud computing. Nowadays, users are able to execute their software applications in remote computing clouds because of the data storage and processing resources can be acquired and released on cloud. In computing clouds, the cloud providers allow the virtualization to “elastically” and promptly respond to client resource demands and requirements [6]. This cloud model consists of five essential characteristics, three service models, and four deployment models.

Although, several benefits are offered by cloud computing, several challenges are resisting the migration of customer software and data into the cloud. The security of the storage and processing of sensitive data on remote machines are even managed by the customers themselves. So, there is a need to provide the security of data on cloud and must be additional control for data security for the fulfillment.

3.1. Issues of Cloud Computing

Most of the current issues for cloud computing are:

Data Security – Many users worry about the remote data on cloud from attackers, thieves, and disgruntled employees.

Reliability – Some users are worrying whether the cloud service provider is financially stable or data storage system is secured.

Ownership or Privacy– Some people are concerning that they could lose some or all of their rights on the cloud storage data. Many cloud providers are addressing this issue with well-managed user-sided agreements.

Data Backup – Cloud providers employ replicated servers and data backup processes, but some data owners are worrying to control their own backups.

Data Portability and Conversion –As the service competition are grown and open standards are established, the data portability issue will ease, and conversion processes will become available supporting the more popular cloud providers. As a

worst case, the cloud subscriber will have to pay additional charges for custom data conversion.

Multiplatform Support – As the cloud-based service integrates across different platforms and operating systems, most of cloud service providers are supported the multiplatform requirements which will ease as more user interfaces become web-based.

Intellectual Property – Most of the company are upgrading their business infrastructure as new and they use cloud services as a core business for global marketing.

3.2. Motivation

Library management in this proposed system provides a convenient along with the increasing knowledge levels by utilizing the advantages of cloud computing.

The requirements of library management are also growing data day by day, causing the library’s resources to be relatively short, to library of a university. Traditional web-based library management in various colleges and universities need to purchase highly for its own database and resources, this is the main flaw of traditional web-based library system. Cloud-based library management system presents new infrastructure and the environment through the cloud computing and it may use resources more effective and can solve the defects of traditional library management system.

3.3. Library Management System

A library management system has been developed to handle basic book-keeping functions of a library on the computerized library data. It’s a well develop management software solution for a library system. It helps to provide digital information on any book present in library to the user as well as staff member from anywhere and anytime. It keeps a track of book issued, returned and added to the library system.

3.4. Cloud Based Library Management System

Cloud computing can share the server in many application procedures, realizes the resources sharing, thus also reduced server’s quantity, achieves the effect of reducing cost.

Software as a Service(SaaS), through the browser to the form of services provided to the applications.

Platform as a Service(PaaS), the form of services provided deployment platform (that includes a database, middleware and development tools, all are in the form of services through the internet) to the developers and application development.

Infrastructure as a Service(IaaS), is the form of services that provide servers, storage and networking hardware devices. Utilizing cloud in the library management system, will obtain a greater efficiency.

3.5. Google App Engine(GAE)

Google App Engine is a platform as a service(PaaS) cloud for developing and hosting web applications under the control of Google-managed data centers. App Engine provides for web applications for global market place so the number of requests will increase for that application. App Engine automatically allocates more resources for the web application to handle the additional demand. Google App Engine allows free of charge a certain level of consumed resources to customer but the additional storage, bandwidth, or hours required by application must be pay charge for the use.

3.6. Developing GAE

Google App Engine(GAE) allows web developers to build applications on the same scalable systems that power Google's own applications. Using App Engine, developers only need to upload an application and there are no need servers to maintain. Apps can be served from own domain name using Google Apps or using a free name on the "appspot.com" domain. Developers can develop scalable applications which are growing from one to millions of users to 5 million because of Google App Engine application has enough CPU, bandwidth, storage to serve for free (additional resources must be pay for use).

Developers can also use prefer programming language on Google App Engine Cloud Platform as shown in figure 1.

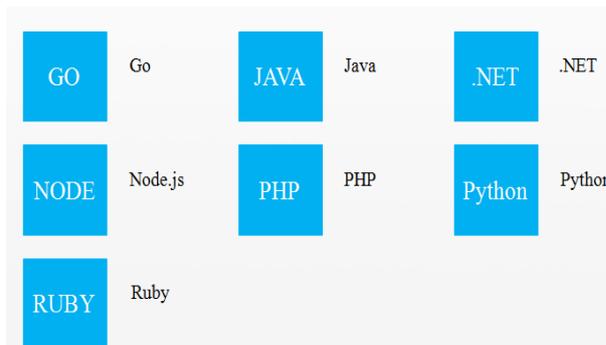


Figure 1. Available Language for GAE

3.7. Benefits of Google App Engine

Advantages of GAE are as described as following:

- Easy to build
- Easy to deploy
- Easy to maintain
- No need to buy server space
- Automatic scalability
- Reliability, performance and security on Google infrastructure
- Cost efficient
- API's to develop applications

4. Access Control Methods in Cloud

Data access control is a mechanism in which users may be granted or denied access to the data for security and privacy of the data and protecting it from the unauthorized and malicious users. Cloud stores massive amount of sensitive information of users that can be shared by other users of the cloud. Hence, this sensitive information must be control for security from the malicious users by using access control mechanisms.

Here, each user and each resource are assigned an identity to the data. So, these methods are called the identity-based access controls. Access control mechanisms are also extensively used in the medical health care, in which access to the sensitive information of patients is granted only to the medical professionals, hospital staff, researchers and policy makers. Data access control is also importance in online social networking [7].

4.1. Mandatory Access Control(MAC)

Mandatory Access Control is the type of secure data access control only the administrator

manages the access control rules. MAC compares the sensitivity level at which the user is working to the sensitivity label of the object being accessed and discard unless certain MAC checks are passed. MAC is mandatory because the labeling of information happens automatically, and ordinary users cannot change labels unless an administrator authorizes them. Sensitivity labels are assigned to files, devices, windows, hosts, networks, and to other system objects that user access [7, 8]

Administrator defined the level of job authority by assigning the upper bound of a set of sensitivity labels at which the user can work. Administrator also defined a minimum responsibility label that is the lower bound. Administrators can manage and control users to work at a single label. In mandatory access control(MAC), the administrators can edit the level of a resource, and no one may grant a right of access in the access control policy. MAC always checks who create, access, and maintain information to follow rules set by administrators. The access control placed on the processing of data (reading or writing or creating or deleting) that are generally accepted when implementing a MAC policy:

- Reading a file; the process level must be dominated the level of the accessed file.
- Writing a file; the process level must be dominated by the level of the accessed file.

4.2. Role Base Access Control(RBAC)

RBAC controls the user accessing to resources based on the user role. A user role is a level of user and the level of permissions needs to accomplish the work of that user role. A user may have a certain role, with each role having a set of access permissions.

The main benefit of role-based access control(RBAC) is flexibility [1, 7]. In RBAC based applications, a user's access grant can be varied by different defined rules. For example, assigning a user's authorization is the removing or adding the privileges associated with a given role.

The granularity of system privilege management related to the RBAC based system as another advantage. The system privileges can be as best as one can choose, the user roles offer their incremental management.

5. Implementation of the System

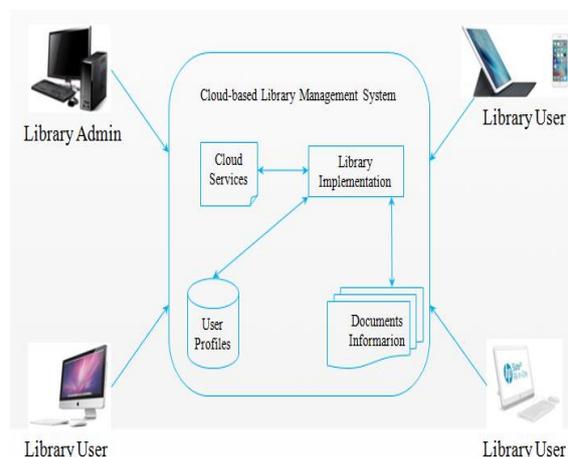


Figure 2. The System Overview

Virtualization and cloud computing are particularly attractive choices for library management system which is challenged by both growth in the size of the indexed document collections and new features. This thesis will present the implementation of university library on cloud computing.

Google App Engine(GAE) technology is used to implement the library management system. Library documents used in this system are collected from the conference papers, text books, referenced books and thesis books of UCSY. As the cloud base library management system has multi-user level, the system also maintains the MAC policy to control the data security for different user accessing.

The proposed system developed for the following reasons:

- To learn cloud computing and cloud computing services which can be utilized in management and security control for university library.
- To implement a cloud-based library management system that can support scalable services to users.
- To support the security control for cloud base library management system to the users from anywhere.
- To save time, cost and space for developing library management system.
- To develop a library system in maintainability and safe.
- To provide right access control based on user's roles that are assigned according to the enterprise's policy decision.
- To maintain the data availability only authorized user with need-to-know.

The process flow of the system is shown in the following figure 3.

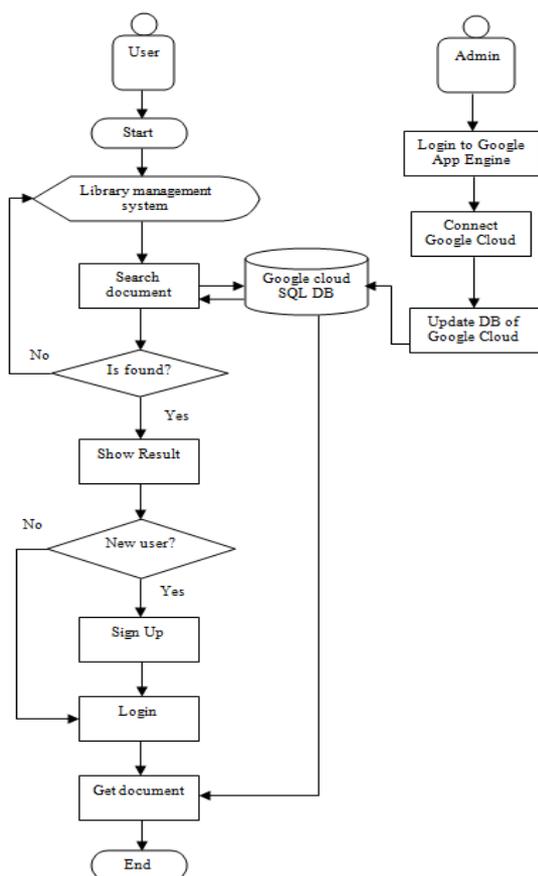


Figure 3. The Process Flow

6. Conclusion

This system presents the implementation of library management of university on cloud computing. Google App Engine is used to implement the proposed system. User service model in university library management is improved by using cloud computing. Using the university library management on cloud, services of libraries will have a new leap in the near future. Services provided by libraries will become user-centric, more professional and more effective etc. Cloud computing is a rapidly developed network environment and it support to the users of high quality and high security. It reduces cost, time, space and maintenance by using the proposed system and users can access services from anywhere.

References

- [1] RajaniKanth Aluvalu, Lakshmi Muddana, "A Survey on Access Control Models in Cloud Computing", Springer International Publishing Switzerland 2015 S.C. Satapathy et al. (eds.), Emerging ICT for Bridging the Future.
- [2] D. Richard Kuhn, Edward J. Coyne, Timothy R. Weil, "Adding Attributes to Role-based Access Control", IEEE Computer Society, vol. 43, No. 6, pp. 79 – 81, (June 2010)
- [3] Jin Li, Gansen Zhao, Xiaofeng Chen, Dongqing Xie, Chunming Rong, Wenjun Li, Lianzhang Tang, Yong Tang, "Fine-grained Data Access Control Systems with User Accountability in Cloud Computing", Proc. 2nd IEEE International Conference on Cloud Computing Technology and Science, IEEE Computer Society, (2010)
- [4] Sushmita Ruj, Milos Stojmenovic, Amiya Nayak, "Privacy Preserving Access Control with Authentication for Securing Data in Clouds", 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, 2012.
- [5] Sushmita Ruj, Amiya Nayak and Ivan Stojmenovic, "DACC: Distributed Access Control in Clouds", International Joint Conference of IEEE, 2011.
- [6] B. Carminati, E. Ferrari, and A. Perego, "Rule-Based Access Control for Social Networks", DICOM, Universit' a degli Studi dell'Insubria, Varese, Italy
- [7] V. Purohit, "Authentication and Access Control", the Cornerstone of Information Security, September 2007.
- [8] National Telecommunications Administration, "Cloud Privacy: Normative Standards Needed to Foster Innovation", U.S. Department of Commerce, Washington, DC 20230, June 1, 2010