iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** IV **Month of publication:** April 2018

DOI: http://doi.org/10.22214/ijraset.2018.4443

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue IV, April 2018- Available at www.ijraset.com

Access Control for Multi-Tenancy in Cloud-Based Health Information Systems

Dr. Sunil Bhutada[1], T.Ramakrishna Reddy[2], S.Shabarish[3], Yaram Anuja[4]
[1] *Professor, Department of Information Technology, Sreenidhi Institute of Science and Technology*
[2, 3, 4] *Under Graduate final year student, Information Technology, Sreenidhi Institute of Science and Technology*

Abstract: ***Cloud computing is a technology that enables access to an extensive pool of shared resources i.e., it offers clients, on-demand access to a huge pool of shared computing resources over networks. It supports cost-effective and highly manageable healthcare systems. The main concepts of cloud computing include multi-tenancy, due to multi-tenancy, there are many privacy and security problems with healthcare information. The models for multi-tenancy and healthcare process are created and then applied role-based access to the users. Basically many hospitals use EHR (Electronic health record) since they are very expensive and tough to manage we are using a cloud to store the records. We used Amazon simple storage service (Amazon S3) to store the records. We have access to respective records for the respective roles. So this resolves the security-related issues that are caused due to multi-tenancy by providing access control.***

Keywords: Multi-tenancy, access control, Amazon S3, cloud computing, health cloud.

I. INTRODUCTION

Cloud computing is a technology that enables access to an extensive pool of shared resources. i.e., it offers clients, on-demand access to a huge pool of shared computing resources over networks. The features of cloud computing include pay as you utilize cost system, location independence, flexibility and scalability, on-demand access and ease of sharing resources. A cloud-based health information system can help reduce cost and contribute to the development of health information systems that are connected, and easily accessible from anywhere, at any time.

Today's health information systems face challenges to manage a tremendous amount of health information of patients. Since EHR systems are expensive and tough to deal with, the healthcare organizations have started to utilize cloud services for health information systems. It reduces the price and contributes to the progress of healthcare systems that are scalable and universally accessible. However, one of the foremost issues of health cloud is security [1, 2, and 9]. As cloud system is used for storing and managing subtle healthcare information, it is important to guard the data against unauthorized access.

Multi-tenancy is one of the main concepts of cloud computing.

It is the idea of sharing one application with various clients. Since data from various users exists in the same location and accessed via the same instance of the service, there is a serious risk of privacy and security problems. Despite multi-tenancy [3, 5] accomplishes better resource utilization in the cloud, it challenges many privacy and security problems by making health cloud vulnerable to attacks. In this, we look into access control problems as introduced by multi-tenancy in a cloud-based healthcare information system.

II. RELATED WORKS

A. Multi-tenancy

Cloud computing provides a concept known as multi-tenancy. While there is a number of definitions exist for the multi-tenant application they remain quite unclear. One definition of multi-tenancy is as follows "Multi-tenancy is a concept of sharing one instance of software/hardware by multiple users."

In this manner, the key parts of multi-tenancy are considered as follows:

1) The ability to share application software/hardware resources [5, 6, 10].
2) The offering of a high degree of configurability of the software [3, 4]
3) The architecture in which multiple tenants use one application and database instance [7, 8].

In a single-tenant environment, the risk of data exposure is moderately little compared to a multi-tenant environment. In multi-tenancy, a security encroachment can bring about the presentation of information to different clients [3, 5].

B. Amazon S3

Amazon simple storage service (Amazon S3) is a storage service offered by Amazon web services (AWS). Amazon S3 is used to store and retrieve data from anywhere with active internet. It provides features like access control, cost optimization, and flexibility. S3 has the ability to accumulate up to 5 TB of data in size with each having up to 2 KB of metadata and objects are being organized into buckets and each bucket is distinguished utilizing a distinctive, user-assigned key within the bucket. Buckets and objects can be created, listed, and retrieved. We can likewise download objects from a bucket. Amazon S3 supports cloud service for storage that has integration from the largest community of third-party solutions and other AWS services.

C. Access Control

Access Control is utilized to guarantee that only approved users can access the data and the system. It is utilized to provide privacy to the user's data by providing the permissions on who can access the data. So here we provided access control to the users to protect the health information of patients by providing access permissions to users in different departments.

III. PROBLEM STATEMENT

Consider a case of access control complications that can transpire in a multi-tenant health cloud. A tenant is an organizational entity and their users who receive services from a cloud service provider. Let us consider an example of a healthcare provider that has several departments such as Radiology, Pharmacy, Insurance, etc. The EHRs belong to different departments and are kept with a cloud service provider and are accessible by users of the respective departments. In order to manage all the departments, a service provider dispatches an application and a database. The problem description explained in Fig. 1. Here we considered the departments of Pharmacy, Insurance, and Radiology. These departments act as tenants that share an EHR database. The database possesses all the records of the patients such as insurance record, medication, diagnostic reports, and condition. The green arrows and red arrows represent authorized to access and unauthorized access respectively. X works as a radiologist and has access to patient condition and diagnostics report. Y is a representative of insurance service department and is authorized to access insurance record from EHR database such as a patient's insurance plan. Z is a pharmacist and is allowed to access medical records of the patient to see a status of medication history and records. All of the users use a SaaS application to access required records. Since many users share a common instance of the database causing multi-tenancy scenario thereby introducing access control vulnerabilities such as:

1) Z, the pharmacist, may check out patient's diagnostic reports and condition.
2) Y, the insurance agent, may check for the patient’s diagnostic reports and medication record.

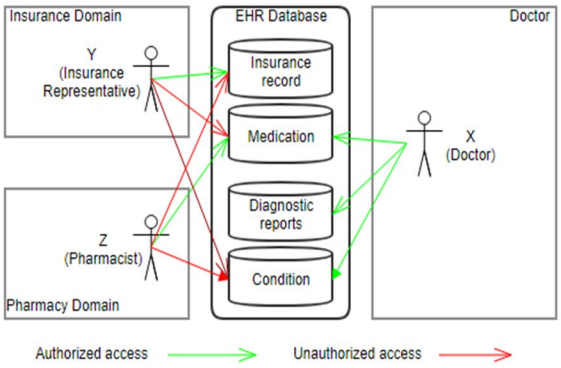


Figure 1: Multi-tenancy in a health cloud

IV. EXPERIMENTS

A. Experimental Setup

We utilized Spring Tool Suite (STS) which is an Eclipse-based advancement condition that is utilized for creating applications. STS provides a ready-to-use environment to implement, run, debug, and deploy your applications. We used Maven and AWS SDK Dependencies of java to develop the application. Apache Tomcat (Tomcat server) which is an open-source Java Servlet Container which is utilized as a server. Amazon S3 is used as cloud storage for storing the records of health information. MySQL database is used to store and retrieve the user information.

We installed java and then STS (Spring Tool Suite) tool to develop the application using java. Now we installed MySQL database and stored the user information. We connected to Amazon S3 using Amazon SDK to store and retrieve records and files. We performed experiments on our environment that runs on Tomcat server.

To model our problem statement in Spring Tool Suite, We created three domains like Radiology, Insurance, and Pharmacy. We created records specific to each domain. For example, medication record is created under Pharmacy domain. So, a user is assigned a pharmacist role and can access medical records. We created users in each of this domain. We assigned a user to roles. We represent healthcare resources as condition, diagnostic reports, medication, and insurance record as records. Each record is owned by one domain. When a record is created, it is created under a specific domain. X, Y, and Z are assigned specific roles and they are the member of specific domains.

V. EXPERIMENTAL RESULTS

We used tomcat server and MySQL database to run the application. It is clarified in the accompanying situations.

A. *Situation 1:* 'X' is a Radiologist and 'A' is a patient. A is diagnosed as having a certain heart condition. A wants to discuss his diagnostic report with X. X checks to read A's diagnostic report in health cloud database. Since X is encountered with A and X is active as a radiologist, X should get permission to read A's diagnostic report.

B. *Situation 2:* 'Y' is an employee of the insurance company and 'A' is a patient. A receives treatment for his heart condition. The treatment history should be written into A's health insurance record. A requests his insurance history. A is encountered with Y and Y is active as insurance service representative, Y should only read insurance record of A but Y should not be permitted to A's diagnostic report.

If Y tries to access the diagnostic report of A then Y gets a message saying that "Access Denied" Fig.2

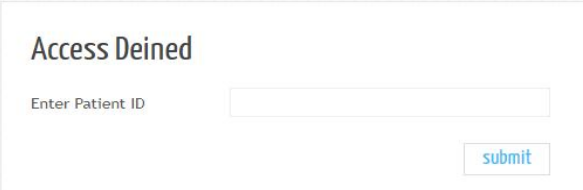


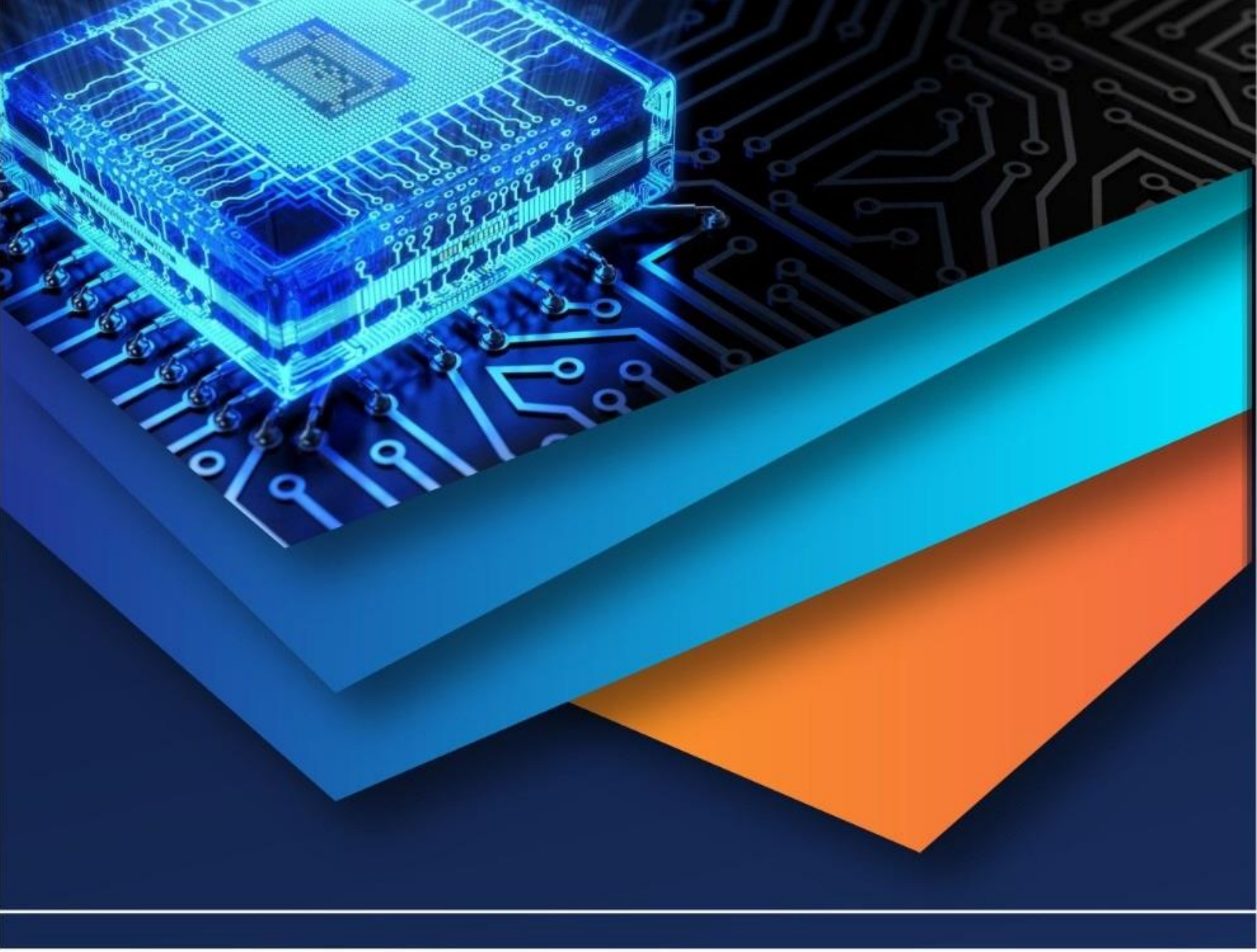
Figure 2: Unauthorized access is denied

VIII. FUTURE SCOPE AND CONCLUSION

In a cloud, due to multi-tenancy, different users and groups try to access sensitive data of patients using cloud services. So the real concerns are access control vulnerabilities. Here we provide privacy and security rules to protect sensitive information from unauthorized access. In this we provided privacy by giving access only to the respective user's i.e.., the access is given based on the roles. This helps the users to access only that specific data for which the individual user is allowed.

REFERENCES

[1] E. AbuKhousa, N. Mohamed, and J. Al-Jaroodi's research paper, "e-Health cloud: opportunities and challenges," and also Future Internet 4, no. 3, 2012, pp. 621-645.
[2] A. Kuo. "Opportunities and Challenges of Cloud Computing to Improve Health Care Services," Journal of Medical Internet Research". Found online
[3] C. Bezemer's research paper. "Performance Optimization of Multi-Tenant Software Systems, His "Ph.D. dissertation, in Delft University of Technology (TU), Delft in 2014.
[4] J.M.A.Calero, N. Edwards, J.Kirschnick, L.Wilcock, as well as M.Wray wrote "Toward a multi-tenancy authorization system for cloud services," in the IEEE Security and Privacy, vol. 8,
[5] Z. H. Wang, B. Gao, C.J. Guo, Z. Zhang W. Sun, and W. H An' research paper, "A study and performance evaluation of the multi-tenant data tier design patterns for service-oriented computing," found in Proc. International Conference e-Business Engineering (ICEBE), in 2008
[6] F.Chong, R.Wolter, and G.Carraro collectively wrote "Multi-Tenant Data Architecture" available online
[7] T. Nguyen, T. Kwok, and L. Lam together published "software as a service with Multi-tenancy support for an electronic contract management application," in the meeting "Proc. International Conf. on Services Computing (SCC).
[8] G.-J.Houben, S.Jansen, and S. Brinkkemper's research paper called "Customization realization in multi-tenant web applications: Case studies from the library sector," in the esteemed conference "Proc. 10th International Conference on Web Engineering (ICWE), LNCS
[9] J. Kabachinski published "What's the forecast for cloud computing in healthcare?" in the reputed "Biomedical Instrumentation & Technology,"
[10] B. Steve and C. D. Weissman together published "The design of the force, com multitenant internet application development platform," in the popular Conference "Proc. 2009 ACM SIGMOD International Conference on Management of data, Rhode Island, USA, June 29-July 02, 2009, pp. 889-896.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY