LUPINE PUBLISHERS

Open Access Journal of Biomedical Engineering and Biosciences

DOI: 10.32474/OAJBEB.2019.03.000157

ISSN: 2637-4579

Review Article

Development of Genomic Data Privacy Protection Model

Adebayo O T[1]* and Fasidi F O[2]

[1]*Department of Information Technology, Nigeria*

[2]*Department of Computer Science, Nigeria*

***Corresponding author:** Adebayo O T, Professor, Department of Information Technology, Nigeria

Received: February 19, 2019 **Published:** February 27, 2019

Abstract

This paper presents a model for securing genomic data in the cloud. The proposed model is a four-level defense mechanism (4ldm) to ensure privacy. Authentication, privacy protection, file encryption, trust behavior of cloud services is modeled for first, second, third and fourth levels of defense respectively. Each level performs its own duty to ensure data privacy and in case one level is deceived by illegal means or malign user enters the system, movement will be made to the next level of defence. The next level of defence will then try to prevent the possible attack until the last level.

Keywords: Cloud Computing; Medical Data; Healthcare; Multi-Level Defense System; Trust Management

Introduction

Cloud Computing Is the Practice of Using A Network of Remote Servers Hosted on The Internet to Store, Manage, And Process Data, Rather Than A Local Server Or A Personal Computer [1]. There Is A Surge of Interest Among Healthcare Companies Regarding the Potential of Cloud Computing and Many Countries Have Started Moving Healthcare-Related Applications Across To Cloud Platforms [2]. Basically, There Are Three Service Delivery Models For Cloud Computing: Software As A Service (Saas) In Which Cloud Customers Use The Provider's Applications Over The Internet, Platform As A Service (Paas) In Which Customers Deploy Their Self-Created Applications On A Development Platform That A Cloud Service Provider Provides And Infrastructure As A Service (Iaas) In Which Cloud Customers Rent Processing, Storage, Network Capacity From Cloud Service Provider. The Cloud Computing Paradigm Is Associated with Security Concerns Both at The Providers' End and Consumers' End. While Providers Want to Ensure That Their Resources and Services Are Utilized Only by Authorized Users; Consumers Would Like To Ensure That Their Data Is Securely Maintained In The Cloud And That The Servers Are Not Compromised. It Is Possible to Facilitate Availability of Genomics Anytime and Anywhere Through Cloud-Based Services If Data Is Stored On The Cloud, But According To [3], A Lot Of Questions Could Be Asked By User: Is My Data Secure In Cloud? Can Others Have Access to My Confidential Data? How Compliant Are Cloud Service Provider to Government Cyber Security Policies And Regulations? What Happens When an Attacker Brings Down Applications Hosted on The Cloud Using Malware And Other Means? This Research Proposes an Integration of Multi-Level Defense Mechanism For Enhanced Security Of Medical Data In The Cloud. Authentication, Privacy Protection File Encryption, And Trust Management Service I.E. Trust Behavior of The Cloud Service for Healthcare Delivery Are Modeled. The Remaining Parts of This Paper Are Structure as Follows: Section 2 Presents the Advantages of Cloud Computing To Healthcare; Section 3 Presents The Proposed Data Security Model For Healthcare Delivery In The Cloud; Section 4 Presents The Conclusion Which Is Drawn From The Findings. Cloud Computing Is Gaining More Popularity, More Organizations and Enterprises Are Moving Towards Cloud, But the Key Concern Has Been Security [4]. Healthcare Industries Are Motivated to Use Cloud Facility Because Healthcare Data Are 'Big Data'. The Various Challenges That Are Peculiar with Volume, Veracity, Variety, Value, Velocity and Variety. Some Advantages That Cloud Storage Offers Over Traditional IT Infrastructure Are

I. Flexibility: Users Can Scale Services to Fit Their Needs, Customize Applications and Access Cloud Services from Anywhere with an Internet Connection.

II. Efficiency: Enterprise Users Can Get Applications to Market Quickly, Without Worrying About Underlying Infrastructure Costs or Maintenance.

III. Strategic Value: Cloud Services Give Enterprises A Competitive Advantage by Providing The Most Innovative Technology Available.

Literature Review

With cloud computing, patients' digitized health information such as medical histories scanned images, blood types, allergies and genomic data can be stored in the cloud and made accessible via secure authentication to people authorized by the patient [5]. Subscribing to a cloud solution for storing and sharing the huge data files can save hospitals, physicians and other organizations in the healthcare value chain heavy up-front investments in high capacity systems, while also boosting speed and efficiency [2]. Medical records and images can be shared with medical practitioners worldwide in real time, treatment and outcomes can be monitored remotely [2]. Medical data gathered by healthcare providers are massive, complex, and difficult to store with traditional IT infrastructure and data management tools. They include clinical data, prescription data of patients, medical images, laboratory data, data from pharmacy and insurance departments, and data gathered from social media sources [1,6]. A (4ldm) can be considered for privacy preservation, each stage performs its own duty to ensure that data security of medical data in the cloud.

Genomic Data

The Genome Contains the Hereditary Information of An Organism. The Human Genome Is Encoded in Deoxyribonucleic Acid Molecules Which We Commonly Known As DNA. DNA Molecules Consist of Two Biopolymer Chains Each of Which in Turn Consists of Nucleotides. These Nucleotides Are Represented As A, C, G, T Which Are the Acronyms of Adenine, Cytosine, Guanine and Thymine Respectively. In DNA, These Nucleotides Form Base Pairs by Making Bonds With Each Other: A Bonds with T and C Bonds with G. There Are 3 Billion Base Pairs in Whole Haploid Human Genome Sequence, Distributed Across 23 Chromosomes. The DNA Of Two Different Individuals Are Almost Identical (99%). In Fact, [7] Showed That DNA Of Two Individuals Differ No More Than By 0.5%. This Small Amount of Variations Distinguishes One Individual from Another. Several Types of Genetic Variations Occur in Human Population, Such as Single-Nucleotide Polymorphism (SNP), Copy-Number Variations (Cnvs), Rearrangement Etc. Single Nucleotide Polymorphism (SNP) Is the Most Common Form of DNA Variation at A Specific Position in The Genome, Which Represents A Difference In A Single Nucleotide. Most of The Snps Do Not Have Any Effect on Human Health. But Some Snps Are Directly Responsible for Developing A Particular Disease in The Human Body. For Genomic data collector (gdc) to have access to genomic information of patients; four levels must be passed through. They are Authentication, privacy protection, Genomic data encryption and Trust management levels.

Model Design

(Figure 1)

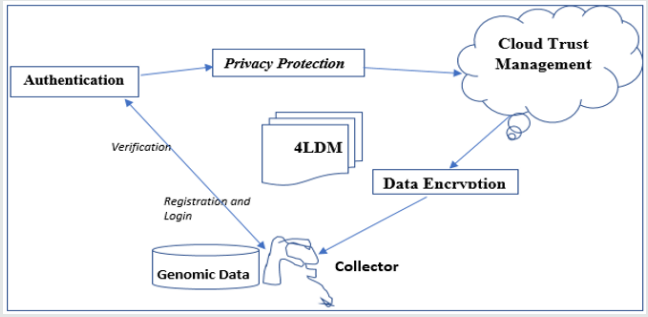

Figure 1: Proposed System Architecture

Authentication (Au)

The Gdc (S) Needs Authentication, Each Must Have Unique ID and Passwords. If the User Authentication System Is Deceived by Illegal Means, And Malign User Enters the System, Then Movement Is Made To Next Level Of Defence.

Privacy Protection (Pp)

Role-based access control (RBAC) can be used as an effective means of privacy protection [8]. The model is built on top of some basic sets, described as follows:

i. U: set of all users (human-being interacting with the cloud services). An element in U can be any convenient representation that uniquely identifies a user in a system

ii. S: set of all services. The system is composed of a collection of services

iii. N: set of all role names

iv. E: set of all environmental constraints

v. O: set of all objects

vi. A: set of all access modes for objects

vii. R: set of all roles. A role is a named job function or title within an organization that is associated with some service; a role is specific to a service [9,10].

viii. P: set of all privilege. A privilege is a right to perform some operation on a particular object. Services confer privileges on their role members and may also recognize the roles of other services. Some definitions are provided [11-13].

Definition 1: A role $r \in R$ is a pair $(s, n) \in S \times N$, where $s \in S$ is a service and $n \in N$ is the name of a role defined by s.

Definition 2: A privilege p ∈ P is a pair (o, a) ∈ O × A, where o ∈ O is an object and a ∈ A is an access mode for the object o. All the elements in Role-based access control (RBAC) can be used to model effective means of privacy protection for medical data.

Genomic Data Encryption (Fe)

Using File Encryptions Allow Complex Mathematical Operations to Be Performed. In This Layer Genomic Data Is Encrypted, Even If the Key was the Illegally Accessed, Through Privacy Protection, Malign User Will Still Be Not Unable To Obtain Effective Access To Information, Which Is Very Important To Protect Business Users' Trade Secrets In Cloud Computing Environment [1].

Trust Management (Tm)

Trust behavior(s)of the Cloud service for healthcare delivery is modeled using equation (1).

$$\frac{\sum_{U=1}^{|\upsilon(s)|} F(U,S) * Q(s,to,t) + X * \Delta(s,to,t)}{|\upsilon(s)|} \quad (1)$$

When User U uses cloud service S, $|\upsilon(s)|$ denotes feedbacks given to the Cloud services. F is a set of feedback (i.e based on several Quality of service (QoS) parameters including availability, security and response time) and tis the timestamps when feedbacks are given [14-16]. $|\upsilon(s)|$ represents the total number of trust feedbacks. $F(U,S)$ are the feedbacks the U users weighted by attacks detection factors. $Q(s,to,t)$ $\Delta(s,to,t)$ is the change rate of trust results in a period of time that allow (TM) adjust results for Cloud services that have been affected by Malicious behavior. X is the normalized weight factor for the change rate of trust results which increases the adaptability. Since trust and identification are closely related, the identity Management Service (idM) can facilitate TMS in detection of attacks against cloud services without breaching the privacy of customer the combination of the proposed (4LDM) can be used to enhance security of medical data in the cloud.

Given That Σ is a Finite Set of DNA Alphabets A(Adenine), C(Cytosine), G(Guanine) And T(Thiamine) Are Set of DNA Characters or Bases.

$$\varepsilon = \{A, C, G, T\} \quad (2)$$

The Four-Level Defense Design for Health Data Privacy Protection in The Cloud Is Represented In Equation (2) As:

$$P = \sum_{i}^{n} \{AU + Pp + Fe + Tm(\varepsilon)\} \quad (3)$$

Where P Is the Privacy Protection, N Is the Number of Individuals Involved.

Conclusion

The benefits of cc to healthcare can never be over emphasized. In this research work, we have carried out an in-depth exploration of cloud computing benefits to healthcare systems. Despite the significant benefits of cc to healthcare, security and privacy of medical data are some of the key challenges and barriers that have led to slow adoption in developing countries and other parts of the world. The proposed model is a multi-level defense mechanism to ensure the security and privacy of patients' medical data. Authentication, privacy protection, file encryption, trust behavior of the cloud service for healthcare delivery are modeled. Each level performs its own duty to ensure that data security but if one level is deceived by illegal means, and malign user enters the system, then movement is made to the next defence. Healthcare sector in developing nations will benefit tremendously from the proposed model for improve services if fully Implemented.

References

1. Michael N, Johnstone (2012) Cloud Security: A Case Study in Telemedicine. Australian eHealth Informatics and Security Conference. School of Computer and Security Science and ECU Security Research Institute Edith Cowan University, Perth, Western Australia.
2. Kayla Searl, (2015) Exploring Thebenefits Of Cloud Computing To Healthcare Industry Global Healthcare Cloud Computing Market, University Of Cologne, Cologne, Germany.
3. Carlos Oberdan Rolim, Fernando Luiz Koch (2010) Patient's Data Collection In Health Care Using Cloud Computing, Second International Conference On Ehealth, Telemedicine And Social Medicine, USA, Washington.
4. Talal H Noor, Quan Z Sheng, And Abdullah Alfazi, (2013) Detecting Occasional Reputation Attacks on Cloud Services School of Computer Sciencethe University of Adelaide, Adelaide SA 5005, Australia
5. Anusha, Sharmini Enoch (2011) Role of Cloud Computing In The Provision Of Healthcarem, Doctors Academy Publicationss, University Of Patras, Greece 1(1).
6. Lisa A Gallagher, (2012) Navigating The Cloud Risks And Protections For Healthcare Data Cloud Computing At HIMSS12 And Beyond: A Primer On The Many Opportunities Available, BSEE, CISM, CPHIMS Senior Director, Privacy And Security HIMSS , Friedrich-Alexander-University Erlangen-Nürnberg, Wetterkreuz 13, Erlangen, Germany.
7. Pita J, Jain M, Ordonez F, Portway C, Tambe M, et al. (2009) Using Game Theory For Los Angeles Airport Security. AI Mag 30: 43-57.
8. Walt Yao, Ken Moodyand Jean Bacon A Model Of OASIS Role-Based Access Control, University of Cambridge, United Kingdom.
9. Diana JP Mckenzie, JD, MBA Parting the Clouds: Negotiation Tips For Healthcare Cloud Computing Agreements.
10. Kevin Sack, (2011) Patient Data Posted Online In Major Breach Of Privacy The New Work Times, Vanderbilt University Medical Center, Nashville, TN, United States of America.
11. Mouleeswaran, Ashok Rangaswamy (2012) Harnessing and Securing Cloud in Patient Health Monitoring, International Conference on Computer Communication and Informatics, p. 10-12.
12. Paillier P, (1999) Public-Key Cryptosystems Based on Composite Degree Residuosity Classes, In Proc. UROCRYPT, pp. 223-238.
13. Canim M, Kantarcioglu M, Malin, et al. (2012) Secure Management of Biomedical Data with Cryptographic Hardware. IEEE Transactions on Information Technology in Biomedicine 16(1): 166-175.
14. Purcell S (2007) PLINK: A Tool Set For Whole-Genome Association And Population-Based Linkage Analyses, The American Journal Of Human Genetics 81(3).
15. Venter JC, Adams MD, Myers EW, Li PW, Mural RJ, et al. (2001) The Sequence of The Human Genome. Science 291(5507): 1304-1351.
16. Https://Www.Ibm.Com/Cloud/Learn/Benefits-Of-Cloud-Computing.

DOI: 10.32474/OAJBEB.2019.03.000157