World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(RESEARCH ARTICLE)

Check for updates

Development of a security model for protecting the privacy of patients in a cloud-based information system

Akomolede Kehinde K. [1], Olowojebutu Akinyemi O [1], Makinde Bukola O [2,*], Okanlawon Kayode [1], Adewale Joseph A [3] and Idris Tajudeen R [1]

[1] *Computer Science Department, The Federal Polytechnic, Ado-Ekiti. Ekiti State. Nigeria.*
[2] *Computer Science Department, Osun State College of Technology, Esa-Oke. Osun State. Nigeria.*
[3] *Multimedia Technology Department, Osun State College of Technology, Esa-Oke. Osun State. Nigeria.*

World Journal of Advanced Research and Reviews, 2024, 21(03), 308–324

Publication history: Received on 17 January 2024; revised on 28 February 2024; accepted on 01 March 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.21.3.0601

Abstract

This work presents a security model in which medical professionals and other users can have access to patient's health data stored in the cloud without knowledge of the identity of the particular patient which the database belongs to. The access control techniques used in this project grants classifier access to patient data, that is to say, it grants access to data based on the role of the data user. Thus, the aim and objective of the project is achieved.

Keywords: Security; Patients; Database; Cloud-based and Information

1. Introduction

Privacy and security of patient's personal information is of great essence in the health sector today. This work is centered on the development of a security model designed to preserve the privacy of patients in a cloud based medical information system by granting an authorized person access to patient's health data without knowledge of the patient's identity. This work majorly focuses on the health care practitioners on the quest to ensure privacy in patient's data. The breach in the privacy of patient's data in the health sector, requires the need for development of a security model in order to back up the physical measures put in place to secure data. Over time, privacy of patient's data in the hospital has become vital as the rate of stigmatization that comes with making such data public is predominantly high and as a result of this stigmatization, patients do not feel free to communicate with medical practitioners. This has led to a downward trend in the quality of care, because ensuring privacy of patient's health data drives the health initiative of any viable clime.

Access control is a technique that enables us to emphasize a selected restriction on access to data/privileges of authorized users. Therefore, identification, authentication and authorization are the three major activities that make up an access control model. The mechanism of access control allows subject (user) to use their credential to identify themselves as legitimate users and help gain access to resources (Nancy A, 2015). There are only two main types of access control: physical and logical. Physicalaccess control limits access to physical information technology assets while logical access limits connections to computer networks, system files and data (Searchsecurity, 2017).

Patients do not feel secure to come and meet medical professionals in the hospital despite the need for them to meet the medical professionals in situation that warrants medical attention, because of stigmatization, embarrassment and discrimination experienced as a result of the health practitioners not protecting their privacy. Therefore, for this reason

* Corresponding author: Makinde Bukola O

information security model were developed. In the development of an information security model, the client server authentication, data masking and access control technique were considered.

Client server authentication is an information security technology that authenticates a particular client to certain information in such a way that the identity of the client is provided to the server using either a username or password. This technology can be used to prevent unauthorized access to information/data, as most organization adopts it for meeting privacy compliancy. The target of privacy in a security system is not just to protect the contents of the message but to protect the identities of communication parties (Liaoliang Jiang, 2018). In this medical information security system, the medical professionals must not know patient's identity at any time. However, the medical professional could be granted access to other health data of the patient.

The background of this work lies on the discomfort that lack of privacy in the health sector brings to patients. The stigmatization caused by not ensuring privacy of patient's health data reduces effective communication between medical practitioners and patient and it leads to a great deal of frustration. Sequel to the rate at which information technology is picking up a huge popularity in our world today, there is a

justifiable need for a more reliable security model in the event of medical information system. This work implements a security model, with the design taking into consideration both real and practical situation and for this reason, a prototype is developed to keep the privacy of patients safe in the cloud and initiate data masking whereby the identity of patients in the data base will be hidden from medical professionals, researchers and the public at large. The purpose of this project is to ensure that patients health data are kept private and secured.

Patients medical data are collected and stored by health care practitioners on a daily base giving rise to huge repositories of medical information. A lot of health care services providers now have their presence on the internet which has revolutionized the world of communication with its attendant's ease in providing better health care services to patients. To be efficient in rendering these life critical services, patient private data containing clinical information are collected and stored when patient-doctor consultation and patients' clinical test results. There is no gain saying that these data on patients left on hospitals' medical information system are used for further research purposes by medical researchers, other healthcare givers, hospital administrators, medical students, etc.

Medical professionals and other healthcare stakeholders need to constantly access patient's status for diverse purposes. Disclosure of patients' health and clinical data breaches the privacy and the protection of their personal sphere of life, hence access to these patients' data should be streamlined to ensure that the private health conditions of patients are not made public or accessed by wrong users which might have debilitating consequences like stigmatization and other psychological trauma. Several

alarms have been raised by patients and there is a justifiable need to address the issue. In a quest to prevent medical professionals and other unauthorized individuals from having knowledge of particular patient's identity which data belongs to, this project "security model for preserving the privacy of patients in a cloud based medical information system" was developed.

The privacy of any patient in a hospital or health institution is dependent on the ability of the health institution to continually preserve the identity and or privacy of such patient in their database to the public so as to avoid stigmatization of any kind on the patient and protect the interest of individual patient. The current methods of securing patient's information in some health institution are manual and inconsistent. Therefore, it is important to preserve the privacy of patients by putting measures in place to ensure that their health data are not linked to their identity using a well secured model because failure to ensure privacy of patient's identity will bring about embarrassment, stigmatization and discrimination of patients regarding employment opportunities and related societal issues and it will also reduce effective communication between medical professionals and patients.

In this work, we propose a privacy preserving protocol or model which leverages on controlling access to patients' health depending on the role and identity of the patient data requester. To achieve this, we explored different access control techniques in information security to determine an appropriate method for implementation. We also aim to protect the patient data in the health information system by a data masking approach integrated with the role and identity- based access control schemes to give us a robust access restriction thereby assuring patients' privacy.

Access control is a way of limiting access to a system or to physical or virtual resources. In computing, access control is a process by which users are granted access and certain privileges to systems and information. In the field of information security, Access Control (AC) is the selective restriction of access to particular information or other resources. Data

masking on the other hand is way of hiding the original data with a modified content such as characters. The usefulness of data masking in this project is to protect data which have been classified as personal information or sensitive data. The model developed in this project provides for the selective protection of privacy that ensures that consultations with a trusted third party on related medical information inquiries are carried out without any giveaway of the patients' privacy concerns.

2. Literature review

It has been difficult to ignore the fact that security and privacy of patient's health data is an important aspect of research and several computing techniques have been proposed for preserving the privacy of patients. However, so many literatures have been reviewed but few related ones shall be discussed in this section below.

Azeez et Al., 2019 carried out a comprehensive analysis on privacy and security issues in a cloud based electronic health system with target on reviewing existing mechanism employed to handle security and privacy issues in electronic health. The method employed in this research considered answering some research questions such as how security and privacy issues in electronic health can be identified, after identifying the issues they went further to find out how those issues identified can be solved to assure the security of electronic health and finally what directions can be given in the future on the privacy and security of electronic health. This research was limited to the fact that no model was developed to solve security issues of electronic health, rather they only gave direction on how data's can be kept private and secured.

Fang Liu, 2018 carried out a research on clustering K anonymity to preserve privacy of wearable internet of things devices. The work proposed a threat model specifically about data sharing process of wearable devices data after which the K- anonymity method was proposed based on clustering in order to preserve the privacy of data, assure the usability of collected data's and also protects against identity disclosure.

Jiang et Al., 2018 carried out a research on communication without name through anonymous identity based encryption and its application in internet of things, this research was similar to that of Fang Liu, 2018 but with different approach. However, it proposed a scheme that ensures privacy of a communication system in such a way that messages are protected by ensuring users anonymity. The work was based on an identity encryption, whereby the metadata of users are protected and this was implemented in JAVA with java pairing based cryptography library.

Chenthara et Al., 2019 reviewed issues of security and privacy preservation of electronic health record with provision of solution in cloud computing. The research considered cyber security when building their security model for electronic health record, with target on investigating what it will require to keep health data secured and private in the cloud arena. The requirement considered in this work include data integrity, data confidentiality, authenticity, accountability, audit, Non repudiation and anonymity all of which works together in harmony to ensure that health information is not altered by someone who is not authorized, health data is prevented from someone who is not authorized, only authorized users is granted access to health data, and the identity of patient is made anonymous.

M.A Alanezi, 2019 developed an intelligent based electronic health care system for the purpose of solving security and privacy issues in Hospitals. A comprehensive analysis was carried out in this work, this analysis cuts across existing methods and models which have been proposed for solving security and privacy issues of electronic health care systems. The work proposed a new intelligent based security and privacy model which maintains and supports the security and privacy of electronic health system after completing the analysis on the existing model. The model was targeted at several security and privacy issues that affect the electronic health environment. The model was designed in such a way that it accepts request via a user interface agent, this user interface agent connects the users to health records. It authorizes user who provides correct user name and password with necessary protocols being defined by the user interface agent. Furthermore, the database was divided into three regions such as environment region, patient region and current medical information region. The environment region is made up of the location and time at which the data was gotten, while the patient region is made up of patient's personal information such as age, status and finally the medical information region is made up of patient's data such as heart rate, operation history and so on.

Pena et Al., 2019 developed a security model for protecting patient data in a mobile health system via a block chain network which allows receiving, sending and integrating data in safe way through a mobile application for mobile health devices in clinics. The security model was made up of three phases, the first phase was for data collection, the second was for data processing and the third phase was for system monitoring.

Insaf Boumezbeur, 2019 carried out a research on privacy preserving access control for sharing health data in cloud environment. The researchers surveyed vital works that are recent on solving the problems of access control and privacy in cloud healthcare system after which they pushed forward a hybrid solution for access control considering RBAC and ABAC models which made available secure, flexible and adaptable access to data. This proposed solution was able to improve cordial relationship between patients and health organizations, but still had some drawbacks.

Misra et Al., 2019 did a critical study with other researchers on cloud based health care management with focus on identifying privacy issues and analyzing their effect on cloud based health care services. Three models were proposed in this work for identifying both the direct and moderating effect of these privacy issues over critical success factors for successfully adopting a cloud based health care services.

This research study is also cantered on the previous research works shown but with better modifications. The use of cloud based medical information system and other techniques such as access control, client server authentication and data masking which has better advantages was used in the process of developing this project and it possesses higher security of data compared to that of (Kanchana, 2015) and (C.A Natividad Peña, 2019) in their application, the privacy of patient is preserved. This work development makes it possible for medical professionals and other authorized user have access to patient's health data without knowledge of the identity of the particular patient which the database belongs to. This design has so many advantages over other published works in terms of cost, complexity in the design and most importantly the fact that the identity of patients is kept private, and it possesses better functionality to the afore mentioned.

3. system analysis and design

3.1. System Design Methodology

For this design, a cloud computing network that employs symmetric key algorithm for its data encryption was considered. The symmetric key algorithm adopted is the Data Encryption Standard. Data Encryption Standard was chosen because of its susceptibility to brute-force attacks owing to its short encryption key. Data Encryption Standard was adopted an industry standard and has been widely used in government, private and public sectors of various industries to secure information. This encryption algorithm prides in its strong internal structure and design techniques. The brute-force prevention framework will act as a new layer of security which uses One-time password to give users secure access and Hash function to generate the DES Key by salting the user's password.

The initial stage of development involves preliminary research to identify the initial requirements which are then implemented and tested. To achieve the set of objectives, HTML (Hyper Text Mark-up Language), CSS (Cascading Style Sheet) and JavaScript (front and back end) was used in designing the interface and interacting with the user and server. WAMP (Windows Apache MySQL PHP) was utilized in generating one-time password and DES key, enforcing password policy and storing user's credentials and performing authentication. The research design is the process of structuring the system understudy following specifications of processing requirements. The objectives are to enable the adequate security of user's information stored in the cloud computing environment which utilizes Data Encryption Standard.

The concept of creating another level of security is by authenticating every user into the cloud environment using One-Time Password mechanism, enforcing password policies and generating the Data Encryption Standard key by hashing the user's password with a random generated salt. All these are channeled towards improving security performance.

3.2. Password Policy

Password policies were enforced to every user of the system in other to provide additional level of security to the Brute force prevention system. These policies must be followed in order to utilize the system else in some situations, the user will be denied access to the system. These policies include:

Every password must contain at least one lowercase, UPPERCASE, digit, and symbols (@#\-_$%^&+=§!.) Minimum length of 8 characters.

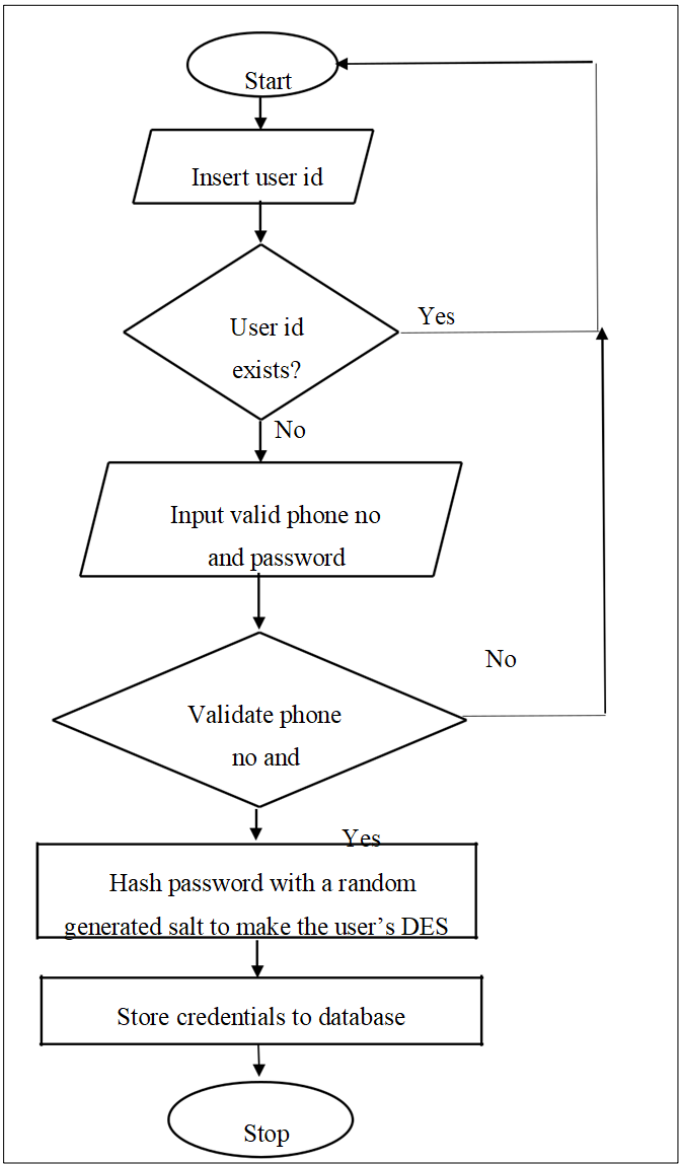
A login attempt of more than five trials, will result in access denial of the account from the user.

A change of password without correctly getting the previous password will result in access denial of the account from the user.

Changing of user's password periodically else the account will be blocked.

3.2.1. Data Encryption Standard Key

Generation of DES key is required for encrypting data in any encryption system that utilizes Data Encryption Standard. In this study, the key is generated by hashing the user's password (which implements the password policies) with a random generated salt value. Following the password policies, the users is required to change the password periodically which in turn generates a new key. This scheme will help in providing the level of security. Password Hashing and One Time Password for the proposed research, the user's password and DES key is hashed utilizing Secure Hash Algorithm 256 (SHA-256) and put away while the Key-Hash Message Authentication Code – Message Digest 5 (HMAC-MD5) will be used to perform a One-Time Password Challenge-Response authentication mechanism utilizing the user's password as key and the unique One Time Password as message for each authentication.



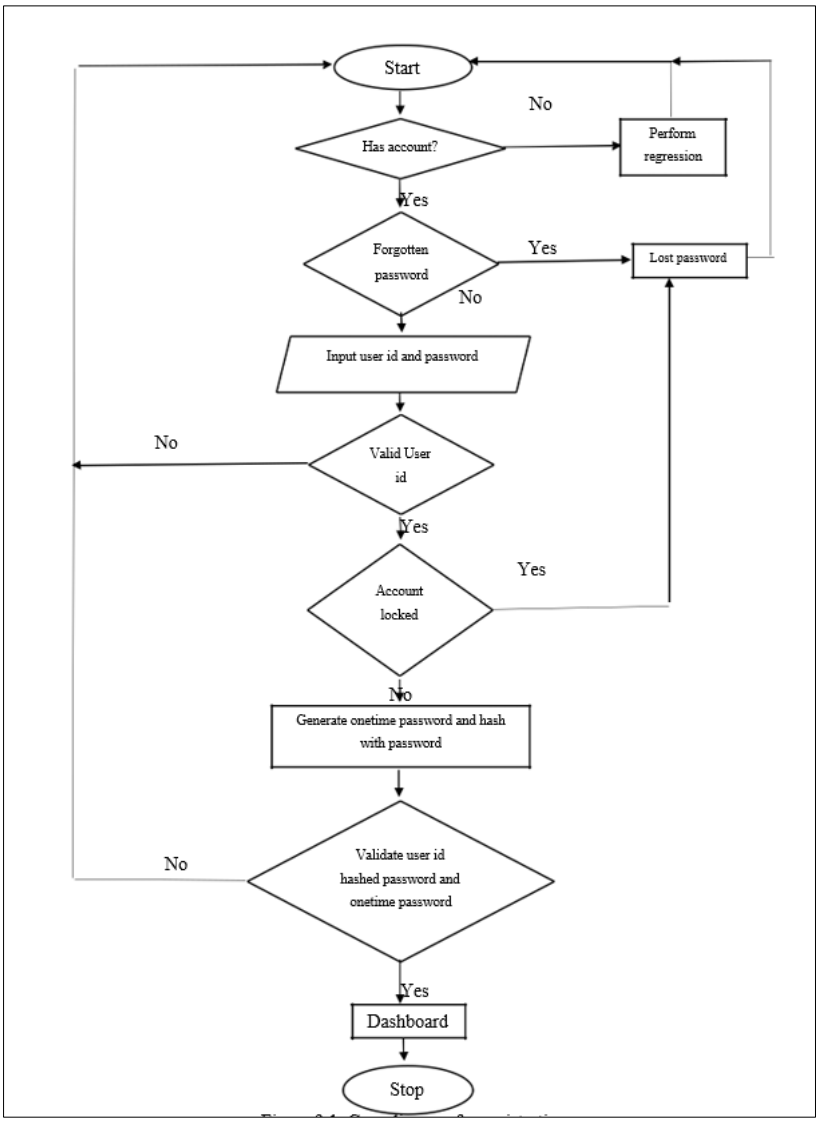


Figure 1 Case diagram for registration

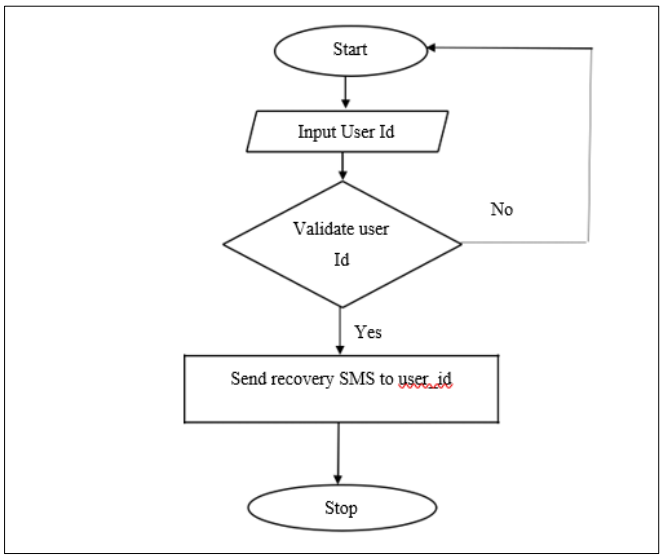


Figure 2 User case diagram for authentication, system analysis and design

3.3. Research Approach

In the development of a cloud based security model for preserving the privacy of patients in a medical information system, the research approach is proposed as follows:

- Designing an architecture of the system that must preserve the identity of the particular patient which the data base belongs to.
- The implementation of the security model must be able to grant access to data based on the role of data users
- The visualization and analysis of the patient's data by medical professionals and other researchers will be visible on either a cell phone or a personal computer.
- The validation of the complete information security system (hardware and software) will be done in a study with several willing participants.

3.4. Overview of the Design

This work start with the acquisition of patient's health data indicating their health status and other relevant medical information of several patients. Following the data sets based on the features it exhibits. Some data masking actions were performed on the acquired data before they were stored in the cloud to protect the data by the developed security model in such a way that the identity of each patient's data in the data sets is hidden to the user. A security model was developed to grant user access to data and preserve the data in the data base using a client server authentication technique, after the development of the security model, a web application was developed to grant either the medical professionals, patients and other researcher/user access to log on to the medical information system from their personal computer or a smart phone device using their unique password. Figure 3.1 shows the block diagram for proposed information security system.

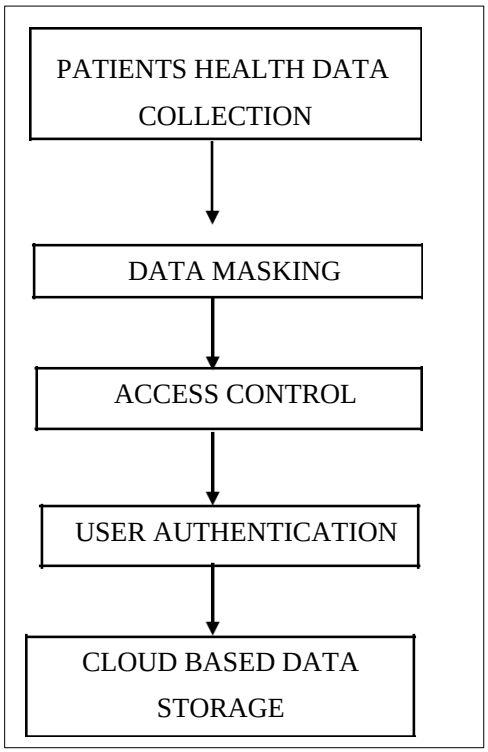


Figure 3 Block Diagram of the developed system

3.4 System architecture

The architecture of the information security model system was developed based on the Wireless Sensor Network method and this is made up of both software and hardware resources; The system has four sections namely: sensing, authentication, displaying and cloud database/storage sections. All sections are to be configured with both software and hardware resources. At the most important part of the system is the user, which is medical professionals, patients and other researchers. The users are granted access to medical information in the cloud based on the authentication of the user. The patient health data generated by sensor is stored in the cloud. This work has the security mechanism inside

the cloud for the purpose of ensuring that the confidentiality, security access control and integrity of the patient's data is kept.

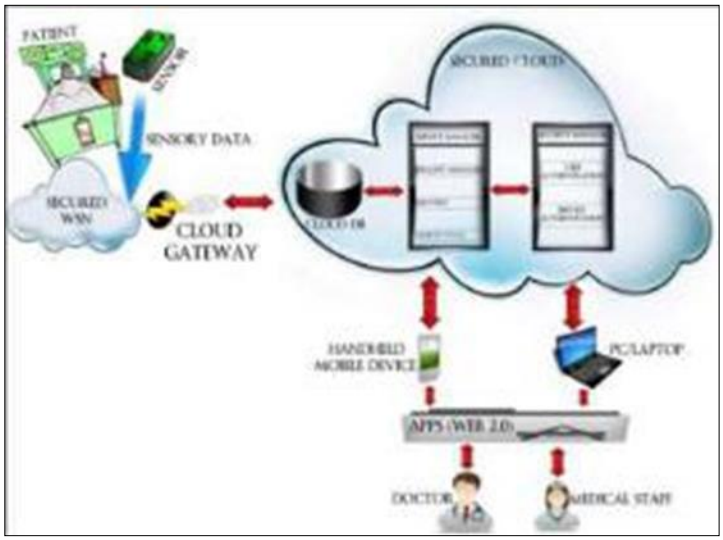


Figure 4 System architecture of the cloud based medical information system (F.A Onik, 2012)

3.5. Design Layout

This work is divided into different section, starting from data acquisition, data masking, access control, user authentication and cloud based data storage.

3.5.1. Data Acquisition

Data acquisition is the first step in the development of a security model in a cloud based medical information system. The data acquired are the medical information of patients. Publicly available data set for all this information's were considered as the data required for this project.

3.5.2. Data Masking

Data masking is the process of protecting the data in the data base. This technique occurs to preserve the privacy of patient's data. The data are being masked in order to make the user not have knowledge of the identity of the particular patient in the cloud database. The data used for the purpose of this project, were masked prior to storing them in the cloud using the local differential privacy data masking technique to ensure that the information in the data base is well secured. We address the privacy-preserving data-sharing problem in a patient health record setting. In this setting, a health institution maintains a patient medical database as a distinct part of a dataset and the aim of this model is to estimate the parameters of a statistical model conditioned on the complete medical data of patients without any revealing any information about the individual patients in their own parts. Our contribution is to classify usage of medical data according to a patient's privacy requirement using local differential privacy, which is a stronger variant of differential privacy where the sensitive medical data of each patient is perturbed with a randomized response mechanism prior to the data access. This is to guarantee the validity and reliability of privacy protection and achieve privacy preserving by adding Laplacian mechanism to handle the expected level of noise added to obfuscate patient health data.

3.5.3. Access Control

Access control was carried out to access data from the cloud using the right access control technique. The access control process was also performed on the model to grant only authorized user access to the cloud database using specific credentials such as user id and password to avoid breach in the privacy of data and it enables us to control how well the data are being accessed by users. Access control is very important because the development of a security model needs an access control mechanism to restrain non authorized user access to data.

3.5.4. User Authentication

At this stage the authentication of users' needs to be verified before being granted access to the data based on the role the data user. This technology ensures that users

are securely identified using a onetime password which grants them access to the cloud where medical information of patients are being stored. As soon as the identity of the user is authenticated, then the system immediately authorizes the user access to the available data. However, if the user is not authorized, then the user is denied access to data.

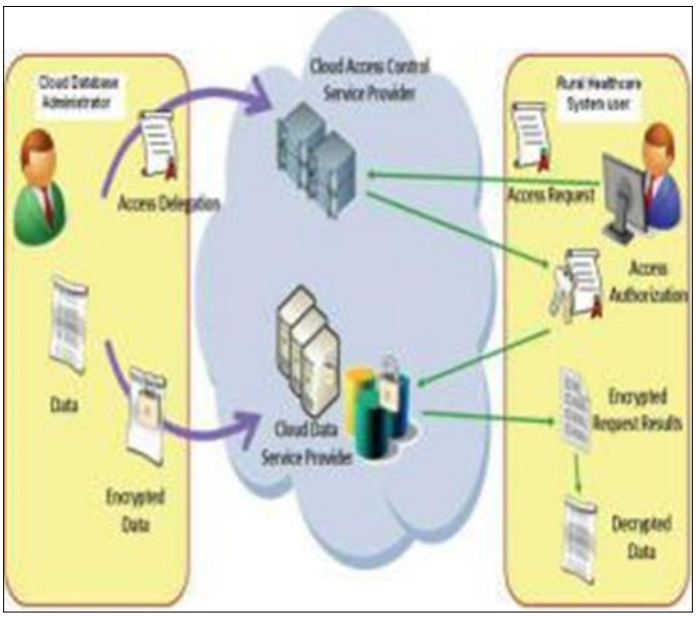


Figure 5 Architecture of an authentication server (R.P Padhy, 2012)

3.5.5. Cloud Database

For storage purpose of this work different medical information of patient's data were stored in the cloud for security purpose. The mechanism of cloud is a network of computers that represents the internet as the cloud. In the bit to improve the information technology infrastructure of medical organization, cloud technology is necessary to provide a secured system. During the implementation of the cloud data base, the cloud services such as Azure and google were considered. An evaluation will be carried out on the performance of the different cloud services used to store data to get the one with the best accuracy.

3.6. Software Components

Working closely with the hardware, the firmware which manage the resources of the embedded processor and an Android application used by the patients or physician to access patient data. On selecting the patient data to be viewed for further analysis, it displays a new layout displaying the data sensed. This is basically collected by sending redundant sequence of bytes containing all data collected in the sensing node to the PDA which serves as the data aggregator and separates each data into distinct constituents which make up the patient's data. The figure 3.4 below shows a proposed view of patient data

Figure 6 Patient data display 3.7 Workflow of the proposed security model

The security model based in a cloud based medical information system works according to the process flow below:

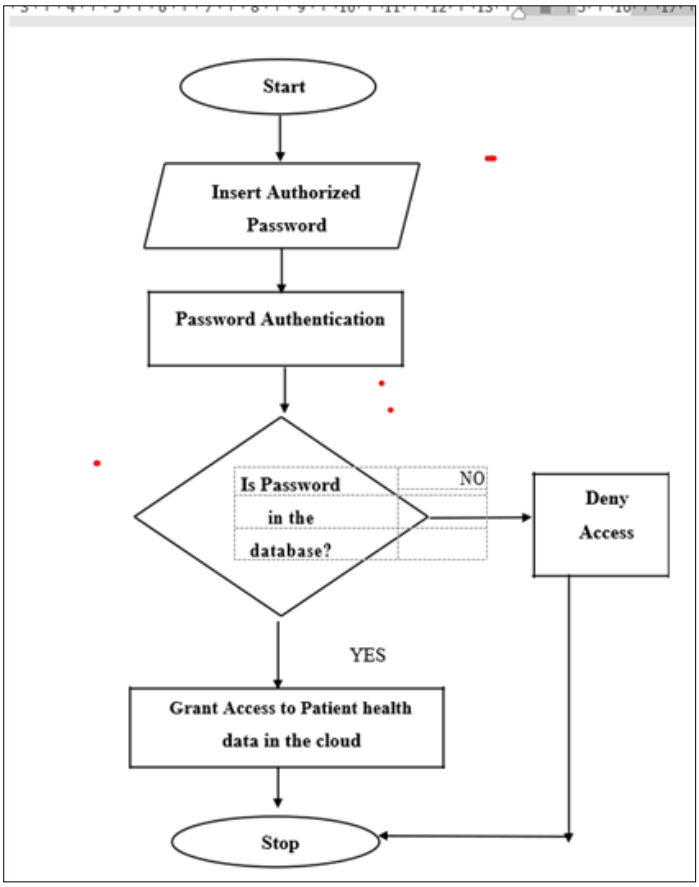


Figure 7 Process flow of access control in the developed security model

The Figure 3.7 above shows the flow chart of the access control in the medical information system. The details of the system are highlighted below:

- Step 1: A user which is either a medical professional, researcher or patient approaches the developed security model using a onetime security password generated by the system to grant only authorized user access to patient's medical information.
- Step 2: The security model reads the password inserted by the user.
- Step 3: After the security model receives the password, it sends it to the database to check its authenticity and confirms.
- Step 4: If the password is authentic, then the user is granted access to patient's health data but if otherwise, the user is denied access.
- Step 5: Once the password is verified, a control signal is generated by the system through which access entry is granted to user.

The onetime password coming from the user is matched with the stored program in the data base. When the password which authenticates a user matches with the stored information, the system grants access to the user.

4. System implementation

4.1. Definition of ε-differential privacy

Let ε be a positive real number and $\mathcal{A}$ be a randomized algorithm that takes a dataset as input (representing the actions of the trusted party holding the data).

Let $\operatorname{im}\mathcal{A}$ denote the image of $\mathcal{A}$. The algorithm $\mathcal{A}$ is said to provide -differential privacy if, for all datasets $_1$ and $_2$ that differ on a single element (i.e., the data of one person), and all subsets of $\operatorname{im}\mathcal{A}$: Differential privacy offers strong and robust guarantees that facilitate modular design and analysis of differentially private mechanisms due to its composability, robustness to post-processing, and graceful degradation in the presence of correlated data.

4.2. Differential privacy implementation

In this work we use the Laplace Mechanism, for implementing Differential Privacy on some function that is to be executed on a database. The Laplace Mechanism accomplishes this by adding noise to the output of f, where the noise is computed under some given parameter as follows:

Let ($_1, _2, _3, \dots, $) be a function on some data in a database = ($_1, _2, _3, \dots, $), for example, can be a function computing the average or the standard deviation on a set of values. Let Δ = Max $'|\ (\ ) - (\ ')|$ over all

neighboring databases x and x '. Thus, Δ is the "sensitivity" of , the maximum difference in values can take on when executed on neighboring databases x and x ', databases that differ in exactly 1 piece of data. For example, if computes the average of a set of values, then Δ = ^{1}, and if computes the standard deviation on a

set of values, then Δ = ^{1} . Finally, let v be the noise added to the output of , where

√

is drawn randomly from the following probability distribution that is symmetric around 0:

$$\Pr[\ ] = \frac{1}{2}\,\frac{-|\ |}{}\quad \text{where} = \frac{\Delta}{}$$

Therefore, the output of executing on some database x is ( ) + .

4.3. Procedure/algorithm in achieving the design goals

This procedure is divided into three stages which includes registration, authentication and password recovery. The procedure concludes that no malicious action was conducted given a straight forward path.

Registration

INPUT: Sign Up

Begin

- Input a valid username, phone number and password (password that follows the password policies given)
- Compare username, phone number and password inputted.
- Compute DES key by hashing the user's password with a random salt.
- Set timer for next change of password, thus change of DES key.
- Return login user and redirects to dashboard. End.

OUTPUT: Login user and redirect to dashboard

- Authentication INPUT: User login Begin
- Input a valid username and password.
- Compare username sent first to server
- Compute row with username and a random one-time passphrase and stores in table on Server
- Return passphrase back to client
- Compute passphrase with password
- Return passphrase with newly hashed password to server
- Compare newly hashed password by hashing password in the table on the Server with passphrase
- When login attempt is more than 5,
- When username and password is invalid, lock account for a period of time.
- Else when username and password are valid
- Return user is logged in.
- Password Recovery INPUT: valid username

Begin

- Input valid username
- Notification is sent to user email,
- Account is unlocked. End.

OUTPUT: account is unlocked

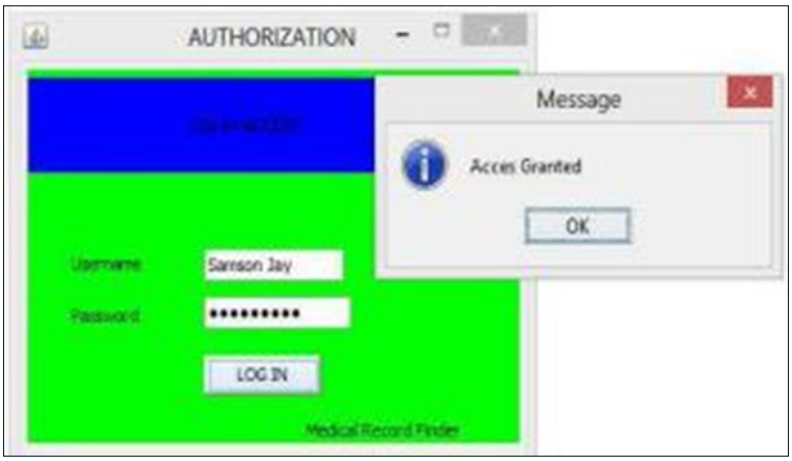


Figure 8 Login interface for an authorized user (A. A. Abayomi-Alli, 2014)

Figure 9 Login interface for an unauthorized user (A. A. Abayomi-Alli, 2014)

4.4. Tools and techniques

Some of the tools needed for this project are as followed:

- Java supported Operating system either Linux, windows or Mac.
- Data Encryption standard key algorithmHypertext mark-up language
- Cascade style sheet
- Java script programming language
- Windows Apache MySQL PHP
- Pre-installed libraries for Visualization, Data reading and model creation.
- Java Integrated Development Environment (IDE)
- Cpabe simulation tool kit
- Average Knowledge of Java programming language

4.5. Simulation result

It is expected that the simulation of the design when carried out using a simulation tool such as *cpabe* toolkit which is an open source package for cryptography, it should indicate that the program is compatible with the system design and that the security model will grant access to only authorized user with the identity of patient hidden in the database.

4.6. Operation of the Model

The proposed security model will operate in such a way that it will receive request through a user interface. The user interface will be connected with the users who for one reason or the other needed to access patient's health data. It works in such a way that it only accepts the username of an authorized user saved in the data base and a onetime password of such users is initiated immediately the system verifies the user name as authentic. The protocols will however be defined by the User Interface which is connected through a website application. This protocols will be defined specifically for the patients or the doctors who are uploading their medical information to the system. Furthermore, the medical information is then stored in a centralized cloud database. The database will be made up of users, roles and their permissions. The authentication mechanism in this design validates the username and password of the user, while the differential privacy technique preserves the identity of patients (M.A Alanezi, 2019).

4.7. Analysis

In the analysis of this work, the expected results gotten from the simulation of this model as well as the real – time testing of the model clearly indicates that the model thrives better in a real life situation. The result shows that access to data is based on the role of the data user and the identity of individual patients in which the data base belongs to is hidden from the user.

4.8. Performance Evaluation

In order to ensure that all the necessary specifications and requirements are met, the performance of the system has to be evaluated according to real life situations. Both the simulation program and the developed security model will be tested in real scenarios by many users. The performance of the system will be evaluated based on the model ability to accurately hide patient's identity in the data base and secure patient's data. The three major metrics that will be used for the performance evaluation are Simulation parameters, accuracy and functional requirements.

4.8.1. Simulation Parameters

In order to ensure that the written program was compatible with the system design, it was simulated. To carry out the simulation, proposed simulation software was used to test the system design.

4.8.2. Accuracy

The accuracy of the system was calculated by comparing how secured it was to store medical information in the cloud with other ways of storage concurrently. The actual error, percentage error (PE) and mean percentage error (MPE), and Percentage Accuracy (PA) will all be computed in calculation of the developed security model.

4.8.3. Functional requirements

The system was evaluated by different users (using both authorized users and unauthorized users), based on its response to grant access and deny access to user, whether or not it saves information after reading the password, whether or not it grants access to authorized user, whether or not it denies an unauthorized user access to data, whether or not it was able to hide the identity of patients which the data base belongs to, data management, theft tolerance, etc.

Table 1 Performance evaluation of access control

Functional requirements	YES	NO
Read Authorized user	YES	
Read unauthorized user	YES	
Grant access to authorized user	YES	
Grant access to unauthorized user		NO
Read more than one user at a time		NO
Save user information		NO
Data management		NO

Generally, according to the various users, the system performance was excellent with zero tolerance to theft and can't be easily manipulated. The model was user friendly, which will enable those that have little or no knowledge about the use of information security system use it. The system is a good anti-theft mechanism and it can be adopted in any organization.

5. Results

To show how well this model performs certain number of features such as personal information of the patient will be incorporated into the model to observe if the model will correctly and accurately hide the identity of the patient in the database and the model is expected to correctly preserve the identity of the patient following the local differential privacy techniques.

Figure 10 Cloud database connection

6. Conclusion

In this work, the front end and back end java script have been used to design the interface which interacts with the user and server, while the windows Apache MySQL PHP have been made useful in the generation of a onetime password system through which authorized users are granted access to the cloud database. The study took into consideration various data masking techniques, client server authentication techniques and several access control techniques. The local differential privacy technique was used to preserve the identity of patients in the cloud based medical information system.

Recommendation

- Several improvements can be made on the system to make it a better security model. It is however recommended that more still be done in the future on;
- Extending this project to develop a similar security model for other aspect of organizations for the purpose of securing data's.
- Implementing this whole project idea as an embedded system in order to allow better flexibility in other field of organization.
- Another security measures such as biometrics aside from a one-time password can be added so as to further strengthen the security of the access control system.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Adebayo A. Abayomi-Alli, A. J.-A. (2014). An Enterprise Cloud-Based Electronic Health Records System. *Journal of Computer Science and Information Technology*, Vol. 2, No. 2, pp. 21-36.

[2] Adeyanju I. A, O. E. (2015). Performance evaluation of Different Support Vector Machine Kernels for Face Emotion Recognition. *SAI Intelligent Systems Conference* (pp. PP 804-806). London: SAI Intelligent Systems.

[3] Anil PD, R. M. (2012). Privacy Preservation Measure using t-closeness with combined l-diversity and k-anonymity. *International Journal of Advanced Research in Computer Science and Electronics Engineering*, Vol 1, issue 8, PP 28-33.

[4] Bai Qing-hai, Z. Y. (2011). Study on the Access Control Model in Information Security

[5] *Cross Strait Quad-Regional Radio Science and Wireless Technology Conference, IEEE*, PP 830-834.

[6] C.A Natividad Peña, A. E. (2019). Security model to protect patient data in mHealth systems through a Blockchain network . *17th LACCEI International Multi-Conference for Engineering, Education, and Technology : Industry, Innovation, And Infrastructure for Sustainable Cities and Communities*, (pp. PP 1-6). Jamaica.

[7] Chen K, L. L. (2011). Geometric data perturbation for privacy preserving outsourced data mining. *ACM Journal of Knowledge and Information Systems*, volume 29, issue no 3, pp 657-695.

[8] Exuberantsolutions. (2016, December 28). Retrieved from http://www.exuberantsolutions.com/smartcard-training.htm.

[9] F. Harmon, R. A. (1989). *Reading between the Lines.* Peterborough, New Hampshire, USA: Helmers Publishing, Inc,.

[10] F.A Onik, S. S.-A.-M. (2012). A Secured Cloud based Health Care Data Management System . *International Journal of Computer Applications*, Volume 49, Issue No.12, PP 24-30.

[11] Fang Liu, T. L. (2018). A Clustering -Anonymity Privacy-Preserving Method for Wearable IoT Devices. *Hindawi Security and Communication Networks*, PP 1-8.

[12] G. Chauhan. (2013). A Review of Privacy Preservation Techniques. International Journal of Engineering Research & Technology, Vol 2, Issue 12, PP 495.

[13] -Gajanayake R, I. R. (2012). Privacy Oriented Access Control for Electronic health record.

[14] James, W. G. (1993). On introducing noise into the bus-contention channel. Proceedings of the IEEE Symposium on Security and Privacy, pp 90–98.

[15] Insaf Boumezbeur, K. Z. (2019). Privacy-preserving access control for sharing health data in cloud environment. The 8th International Seminary on Computer Science Research at Feminine, (pp. PP 25-31).

[16] Jain A. K, R. A. (2004). An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technologies, Vol 14, Issue no 1, PP 1-66.

[17] Jemal Hanen, Z. K. (2016). An enhanced healthcare system in mobile cloud computing environment. Vietnam Journal of Computer Science, PP 267–277.

[18] Juels A, R. R. (2003). The Blocker Tag: Selective Blocking of RFID Tags for ConsumerPrivacy. CCS'03. Washington, DC, USA: 9.

[19] Abouelmehdi, A. B.-H. (2018). Big healthcare data: preserving security and privacy. Journal of big data, PP 1-18.

[20] Kanchana, R. V. (2015). Security Model for Healthcare Application In Cloud Computing. International Journal of Computer Science and Engineering Communications, Vol.3, Issue 2, PP 627-635.

[21] Kato Mivule. (2012). Utilizing Noise Addition for Data Privacy an overview. Computer science department, Bowen University.

[22] Liaoliang Jiang, T. L. (2018). Anonymous Communication via Anonymous Identity-Based Encryption and Its Application in IoT. Hindawi Wireless Communications and Mobile Computing, PP 1-8.

[23] M.A Alanezi, Z. F. (2019). Intelligent based E-healthcare Systems: Towards Security and Privacy . International Journal of Computer Science and Network Security, Vol 19, Issue No 3, PP 16-23.

[24] Maulik Parekh, S. B. (2015). Designing a Cloud based Framework for HealthCare System and applying Clustering techniques for Region Wise Diagnosis. 2nd International Symposium on Big Data and Cloud Computing: Procedia Computer Science (pp. PP 537 – 542). Elsevier B.V. .

[25] Mijanur Rahman, S. N. (2016). Biometric student registration and verification system.1-3.

[26] Milyaev, S. B. (2013). Image binarisation for end-to-end text understanding in natural images.

[27] Mu-Hsing KUO, A. K. (2013). IT Intelligence Cloud Computing for Health Information Management. Health management.org, Volume 13, Issue 2, PP 1.

[28] N.A Azeez, C. V. (2019). Security and privacy issues in e-health cloud-based system: A comprehensive content analysis. Egyptian Informatics Journal, PP 97-108.

[29] Nguyen. (2019, June 30). Understanding differential privacy. Retrieved from towrads data science: http://www.towardsdatascience.com

[30] O.P Chaurasia. (2012). An Approach to Fingerprint Image PreProcessing. International Journal of image Graphics and Signal Processing, Vol 6, issue no 5, PP 29-35.

[31] R.P Padhy, M. R. (2012). Design and Implementation of a Cloud based Rural Healthcare Information System Model. Universal journal of applied computer science and technology, Vol 2, issue 1, PP 149-157.

[32] Ravikumar G K, B. J. (2011). Design of Data Masking Architecture and Analysis of Data Masking Techniques forTesting. International Journal of Engineering Science and Technology, Vol. 3 No. 6, PP 5153.

[33] Chenthara, K. A. (2019). Security and Privacy-Preserving Challenges of e-Health Solutions in Cloud Computing. IEEE Access, Vol 7, PP 74361-74382.

[34] Naisha Sultana, G. R. (2014). CLOUD-BASED DEVELOPMENT OF SMART AND CONNECTED DATA IN HEALTHCARE APPLICATION. International Journal of Distributed and Parallel Systems, Vol 5, issue no 6, PP 1-11.

[35] Shoewu, O. I. (2012). Development of attendance management system using biometrics. The pacific journal of science and technology, Vol 13, issue 1, PP 300-307.

[36] Simson L. G, J. A. (2005). RFID privacy: An overview of problems and proposed solutions. IEEE Security and Privacy, Vol 3, issue 3, PP 34–43.

[37] Stallings W, B. L. (2008). Computer Security. Principles and Practice.

[38] ubhas C. Misra, A. K. (2019). Cloud-based healthcare management: Identifying the privacy concerns and their moderating effect on the cloud-based health-care services. Indian Institute of Technology (pp. PP 1-18). Kanpur India: John Wiley & Sons, Ltd.

[39] Vinoth kumar, S. (2016). A Brief Survey on Privacy Preserving Techniques in Data Mining . IOSR Journal of Computer Engineering, Volume 18, Issue 4, PP 47-51.

[40] Wenrong Z, Y. Y. (2014). Content-Based Access Control: Use Data Content to Assist Access Control for Large-Scale Content-Centric Databases. IEEE International Conference on Big Data, PP 701-710