# A NOVEL METHOD FOR OUTSOURCE MEDICAL DATA SECURELY

**[1]B RAMANA,[2]T CHANDRAKANTH,[3]G SREERAMULU,[4]PRAJAPATHI ALVIN RAMACHANDRA**

[1,2,3] *Assistant Professor,*[4]*Student*

*Department Of CSE*

*Bheema Institute of Technology and Science, Adoni*

**ABSTRACT_** Medical imaging is crucial for identifying diseases, and strict security and privacy regulations need to be implemented because of the sensitive nature of these pictures. For Healthcare Industry 4.0, medical pictures in cloud-based medical systems should be safeguarded before being outsourced. Nevertheless, processing queries over encrypted data without first completing the decryption stage is presently both challenging and impracticable. In the study, we provide a practical way to find the exact closest neighbour among a collection of encrypted medical images. Rather of calculating the Euclidean distance, we may reject candidates by determining the lower limit of the distance, which is connected with the data's mean and standard deviation. Unlike most other current algorithms, our method is able to locate the exact closest neighbour instead of an approximation. Next, we evaluate our proposed approach to demonstrate its efficacy.

## I. INTRODUCTION

In a deployment of cloud computing, which is increasingly common in modern society [1], the owner of the data can outsource databases and administration functions to the cloud server. The latter maintains the databases and offers access controls for managing and querying the contracted database. This lowers the cost of data administration while enhancing service levels for data owners. The cloud, however, might not be completely trusted because it could leak private data to unauthorised parties (such as compromised) or foreign government agencies. [2]

Personal health records (PHR) are becoming the de facto norm for exchanging health information. A PHR paradigm enables a user (patient) to create, manage, and control health data in one central location using web technology, which has improved the efficiency of information storing, retrieval, and sharing. Here, each patient is given complete access to their medical records and is able to share that information with a wide range of users, such as family members, friends, and medical report providers. Although it is simpler to provide PHR services to everyone, there may be numerous security and privacy problems that could hinder its adoption. The primary cause of concern is whether patients can restrict the sharing of their protected health information (PHI), particularly when it is held on external servers where users might not be completely confident. The external cloud storage servers are frequently vulnerable to different attacks, which could make PHI vulnerable, on the other hand, because of the sensitive health information (PHI) that is stored on them. It is essential to establish a fine data access control architecture that functions with untrusted servers to ensure users' (patients') secret control over their own PHRs.

The fundamental concept is to encrypt the data before storing it on the cloud. Here, the PHR owner essentially should be able to choose how to encrypt files and whether or not to grant certain users access to each file. Users who are provided the decryption key must be the only users with access to a PHR record file; all other users must be prohibited from viewing it. The patient shall always be able to request authorization when they deem it necessary, in addition to having the right to always allow for it. The amount of scalability in a PHR system, however, frequently puts patient-centric privacy in jeopardy. The PHR may need to be retrieved by the certified users for either their own usage or authorised use. On the other hand, unlike the single data owner type that is frequently taken into account in the majority of earlier studies, a PHR system has many users who may encrypt according to their own conceivable ways, by employing distinct sets of cryptographic keys. Since patients aren't always online, allowing each user to obtain keys from every owner who’s PHR desires to be read would limit access. Therefore, another option would be to use a central authority to handle all of the key management for all PHR owners, but this again necessitates a high level of authority confidence.

## 2. LITERATURE SURVEY

### 2.1 A new general framework for secure public key encryption with keyword search

Public Key Encryption with Keyword Search (PEKS), introduced by Boneh et al. in Eurocrypt’04, allows users to search encrypted documents on an untrusted server without revealing any information. This notion is very useful in many applications and has attracted a lot of attention by the cryptographic research community. However, one limitation of all the existing PEKS schemes is that they cannot resist the Keyword Guessing Attack (KGA) launched by a malicious server. In this paper, we propose a new PEKS framework named Dual-Server Public Key Encryption with Keyword Search (DS-PEKS). This new framework can withstand all the attacks, including the KGA from the two untrusted servers, as long as they do not collude. We then present a generic construction of DS-PEKS using a new variant of the Smooth Projective Hash Functions (SPHFs), which is of independent interest.

### 2.2 Searchable symmetric encryption: Improved definitions and efficient constructions

Searchable symmetric encryption (SSE) allows a party to outsource the storage of his data to another party in a private manner, while maintaining the ability to selectively search over it. This problem has been the focus of active research and several security definitions and constructions have been proposed. In this paper we begin by reviewing existing notions of security and propose new and stronger security definitions. We then present two constructions that we show secure under our new definitions. Interestingly, in addition to satisfying stronger security guarantees, our constructions are more efficient than all previous constructions.

Further, prior work on SSE only considered the setting where only the owner of the data is capable of submitting search queries. We consider the natural extension where an arbitrary group of parties other than the owner can submit search queries. We formally define SSE in this multi-user setting, and present an efficient construction.

### 2.3 Public Key Encryption with Keyword Search based on K-Resilient IBE

Abstract. An encrypted email is sent from Bob to Alice. A gateway wants to check whether a certain keyword exists in an email or not for some reason (e.g. routing). Nevertheless Alice does not want the email to be decrypted by anyone except her including the gateway itself. This is a scenario where public key encryption with keyword search (PEKS) is needed. In this paper we construct a new scheme (KR-PEKS) the KResilient Public Key Encryption with Keyword Search. The new scheme is secure under a chosen keyword attack without the random oracle. The ability of constructing a Public Key Encryption with Keyword Search from an Identity Based Encryption was used in the construction of the KR-PEKS. The security of the new scheme was proved by showing that the used IBE has a notion of key privacy. The scheme was then modified in two different ways in order to fulfill each of the following: the first modification was done to enable multiple keyword search and the other was done to remove the need of secure channels.

## 3. PROPOSED SYSTEM

In the study, we analyse and provide a secure and effective solution to the precise closest neighbour search problem using encrypted medical images. Our system allows for dynamic updates. It enables data users to quickly add or remove medical photos as needed.

Permitted users should transmit their queries to the cloud for examination after encryption in order to safeguard query privacy. Even when the data and queries are encrypted, the cloud (or a malevolent insider) can learn personal information about the actual data items by examining the data access patterns.

Data encryption by the data owner is an amateurish approach to protecting privacy [7], but it does protect cloud-outsourced data from unauthorised users. Permitted users should transmit their queries to the cloud for examination after encryption in order to safeguard query privacy.

In the paper, we suggest an effective method for locating the precise nearest neighbour in a set of encrypted medical photos. By obtaining the lower bound of the Euclidean distance, which is correlated with the mean and standard deviation of the data, we can eliminate candidates instead of computing the Euclidean distance..

### 3.1 IMPLEMENTATION

### 1. Data Owner

In this module, the data owner Collect Patient data and Upload to Cloudlet like pid, pname, paddress, pcno, pemail, ppulse, pecg, pSymptoms, browse and attach about symptoms with Digital sign, add pimage(Encrypt all parameters except pname) and View all patient collect data in enc format with digital sign.

## 2. Server A

The **s**erver-A manages which is to provide data storage service for the wearable devices and also View all patients and authorize and View all doctors and authorize ,View all patient Cloudlet data with enc format ,View Patient data access request and authorize ,View all Cloudlet Intruders details and View patient details recovered details ,View No.Of same symptoms in Chart(Symptom name vs No. Of Patients), View No.Of Patients refered same doctor in Chart (Doctor Name vs No.Of Patients).

## 3. Data User

In this module, the patient Register and Login, View profile ,Request Data Access permission from cloudlet and view Response, Access Your data and select doctor from combo box and send to corresponding doctor and View doctor response with Medical prescription, Verify your data and recover and View and delete your details.

## 4. Server-B

The Server-B is the one who will perform the following operations such as Register and Login, View Profile, View patient details and give solution like Medicine details, Medical prescription details View all patient Medical prescription Details.

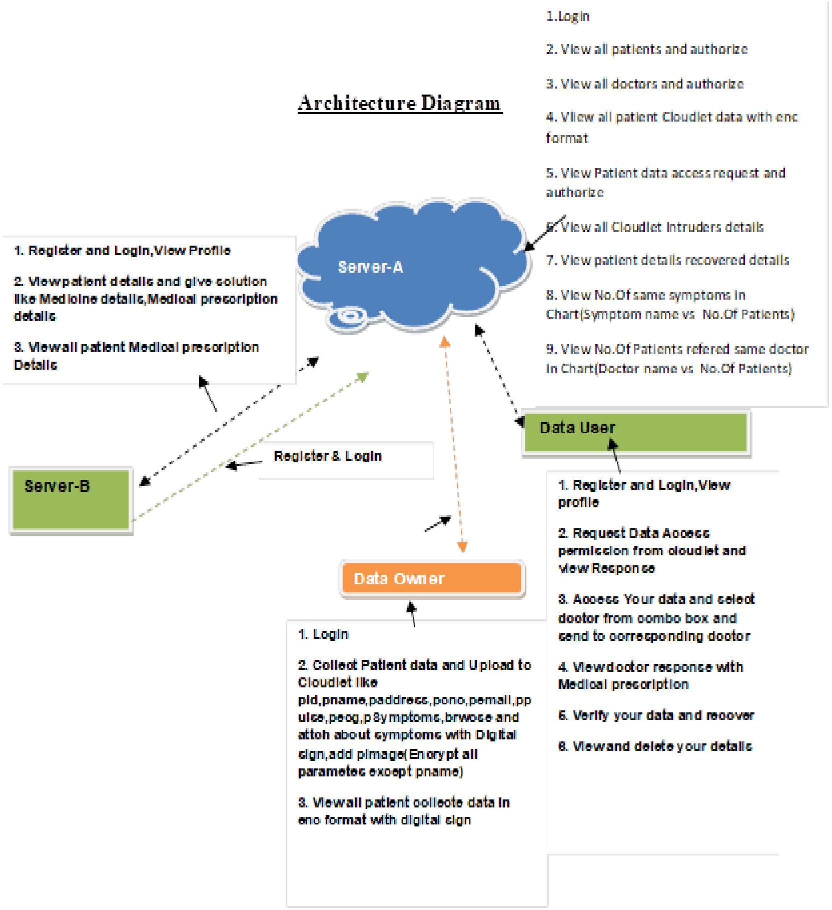
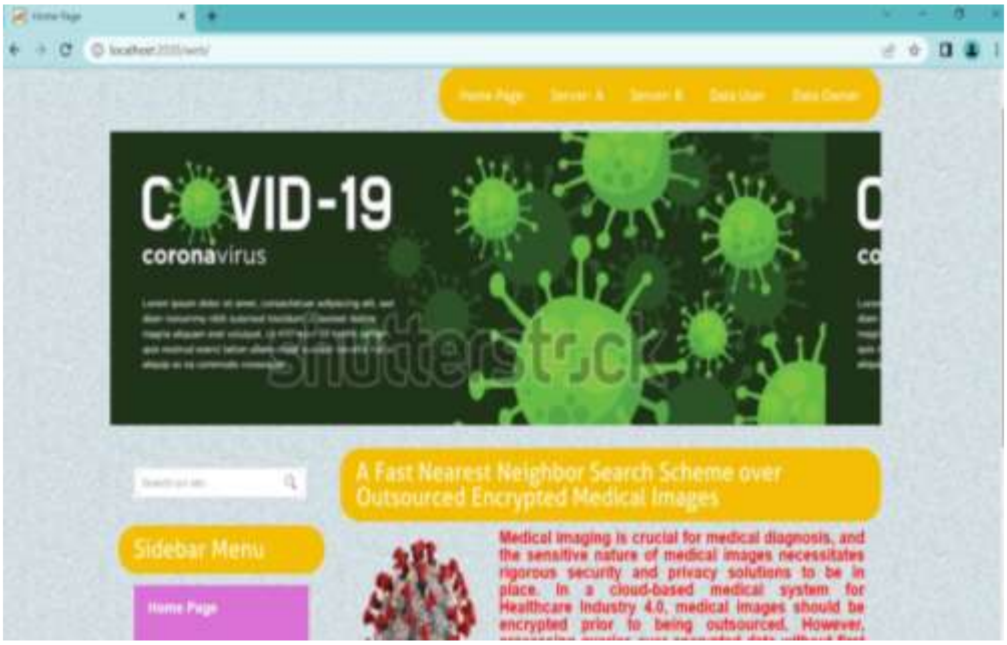

1.Login
2. View all patients and authorize
3. View all doctors and authorize
4. Viiew all patient Cloudlet data with enc format
5. View Patient data access request and authorize
6. View all Cloudlet Intruders details
7. View patient details recovered details
8. View No.Of same symptoms in Chart(Symptom name vs No.Of Patients)
9. View No.Of Patients refered same doctor in Chart(Doctor name vs No.Of Patients)
Architecture Diagram
1. Register and Login,View Profile
2. Viewpatient details and give solution like Medioine details,Medioal presoription details
3. Viewall patient Medioal presoription Details
Server-A
Data User
Register & Login
Server-B
1. Register and Login,View profile
2. Request Data Acoess permission from cloudlet and view Response
3. Acoess Your data and select dootor from oombo box and send to oorresponding dootor
4. Viewdootor response with Medioal presoription
5. Verify your data and reoover
6. Viewand delete your details
Data Owner
1. Login
2. Colleot Patient data and Upload to Cloudlet like pid,pname,paddress,pono,pemail,ppulse,peog,pSymptoms,brwose and attoh about symptoms with Digital sign,add pimage(Enorypt all parametes exoept pname)
3. Viewall patient colleots data in eno format with digital sign

**Fig 1: Architecture**

## 4. RESULTS AND DISCUSSION



A Fast Nearest Neighbor Search Scheme over Outsourced Encrypted Medical Images

Medical imaging is crucial for medical diagnosis, and the sensitive nature of medical images necessitates rigorous security and privacy solutions to be in place. In a cloud-based medical system for Healthcare Industry 4.0, medical images should be encrypted prior to being outsourced. However,

**Fig 2: Showing Home page**

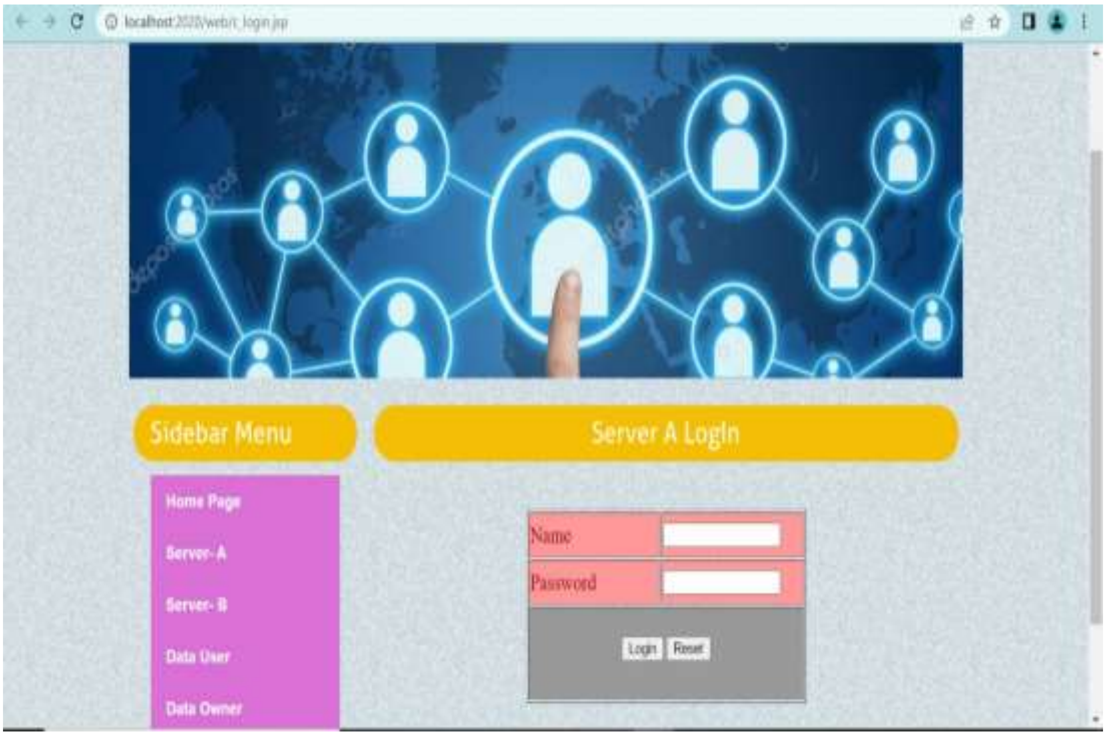


**Fig 3: Showing Server A Login page**

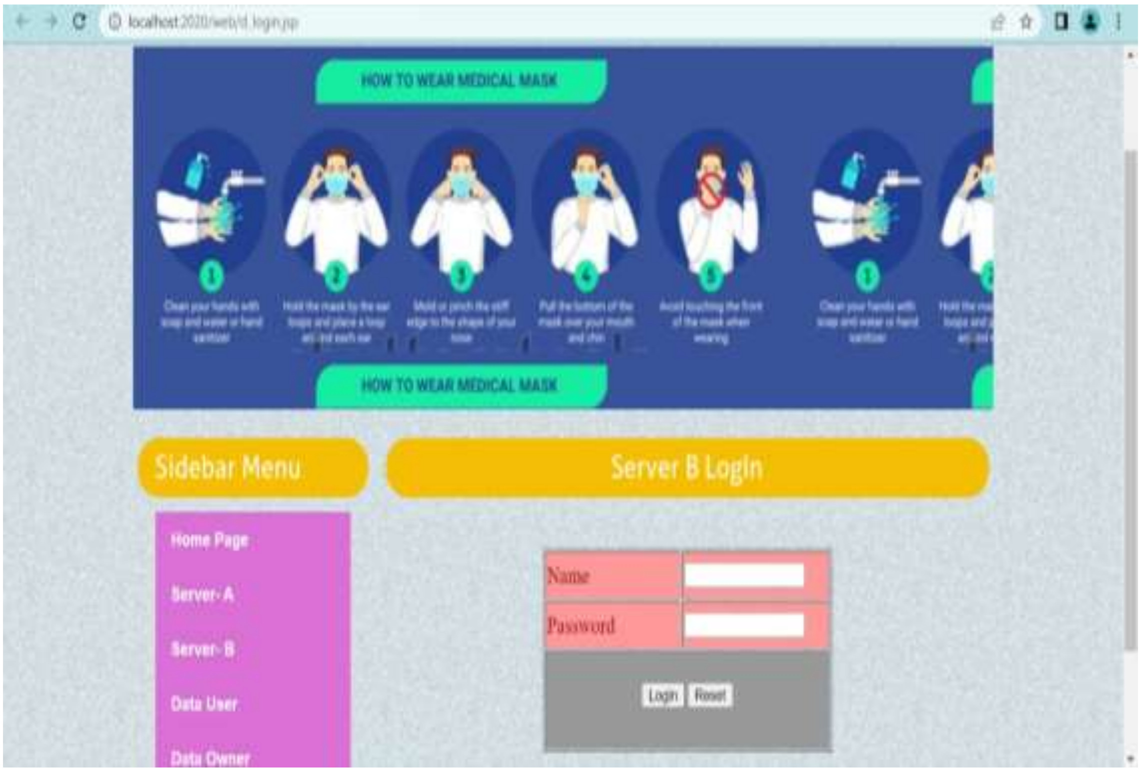

localhost:2020/web/d_login.jsp
HOW TO WEAR MEDICAL MASK
1
Clean your hands with soap and water or hand sanitizer
2
Hold the mask by the ear loops and place a loop around each ear
3
Mold or pinch the stiff edge to the shape of your nose
4
Pull the bottom of the mask over your mouth and chin
5
Avoid touching the front of the mask when wearing
HOW TO WEAR MEDICAL MASK
Sidebar Menu
Server B Login
Home Page
Server- A
Server- B
Data User
Data Owner
Name
Password
Login
Reset

**Fig 4: Showing Server B Login page**

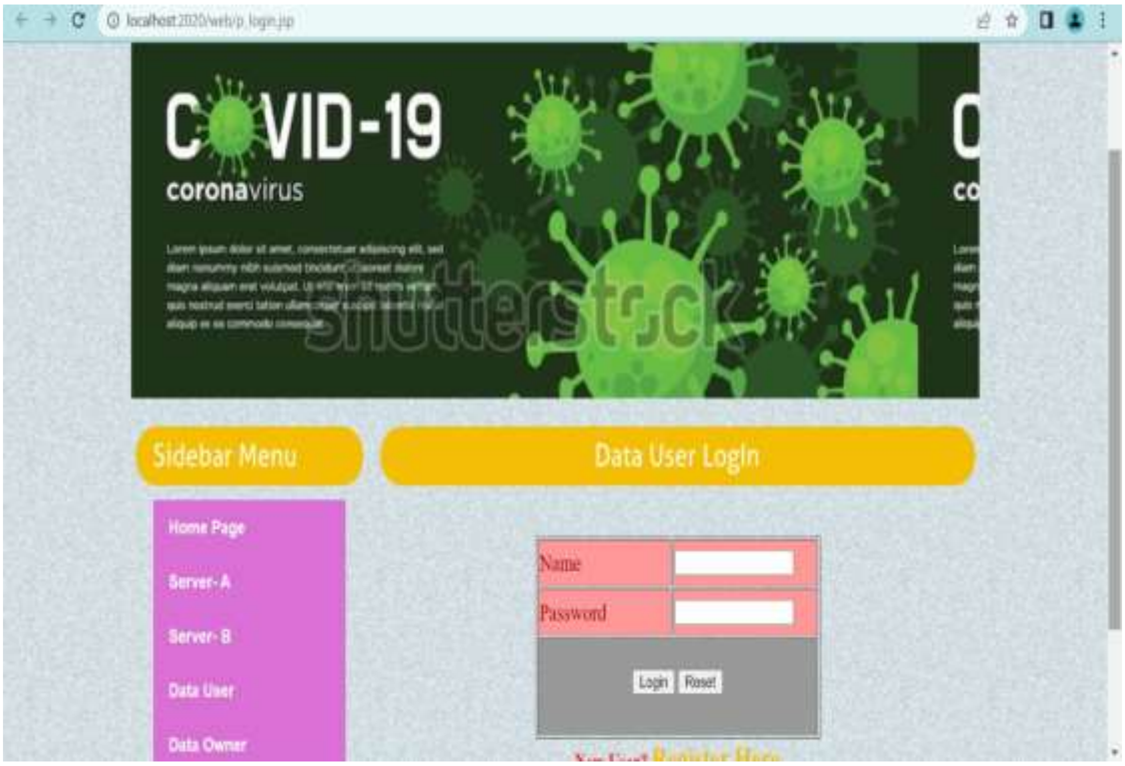


**Fig 5: Showing Data User Login page**

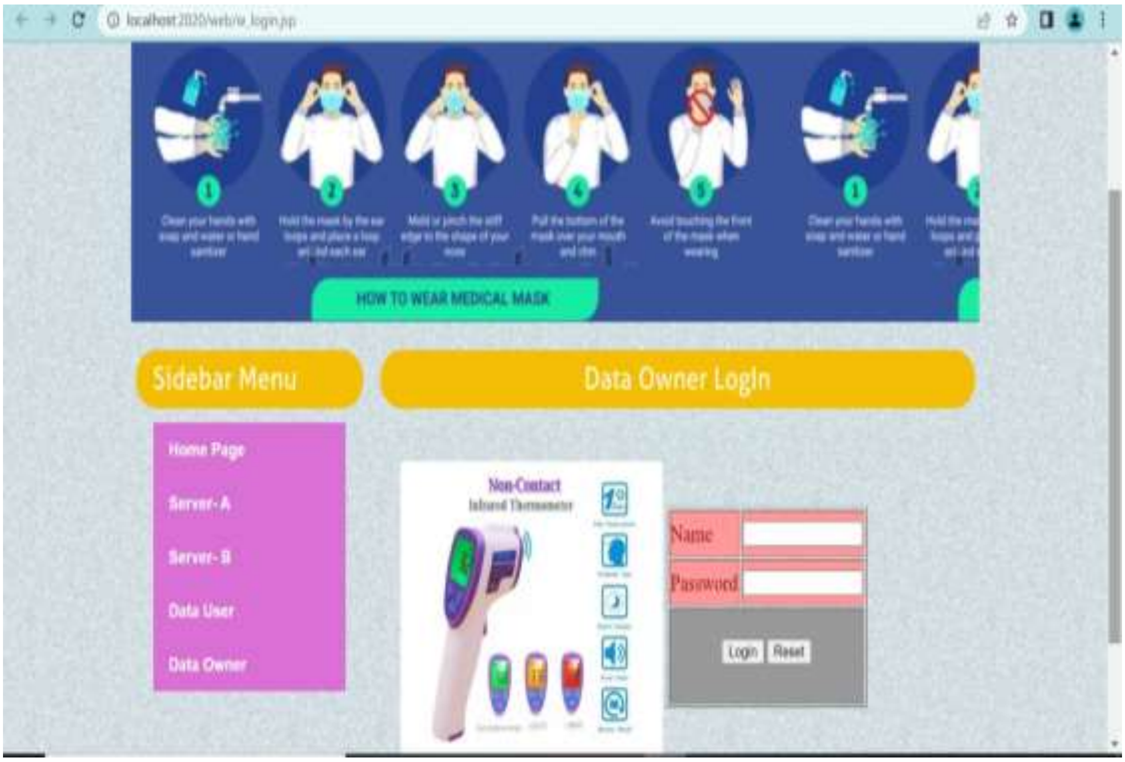

localhost:2020/web/w_login.jsp
Clean your hands with soap and water or hand sanitizer
Hold the mask by the ear loops and place a loop around each ear
Mold or pinch the stiff edge to the shape of your nose
Pull the bottom of the mask over your mouth and chin
Avoid touching the front of the mask when wearing
HOW TO WEAR MEDICAL MASK
Sidebar Menu
Data Owner Login
Home Page
Server-A
Server-B
Data User
Data Owner
Non-Contact Infrared Thermometer
Name
Password
Login
Reset

Fig 6: Showing Data Owner Login page

## 5. CONCLUSION

Cloud-based electronic health record systems will become more and more common as a result of their ability to exchange and access data in real-time across organisations (such as physicians and healthcare providers) and countries. One process becomes challenging, if not unfeasible. In the paper, we outlined a secure and efficient way to use encrypted medical images that are kept on a distant cloud server to locate the exact neighbour. In order to filter out candidate data points, our technique securely computes the lower limit of the squared Euclidean distance between a database data point and the query entered by an authorised user. We evaluate the performance of our method using real medical pictures. Future research will include locating a real-world healthcare organisation to develop and implement a prototype of our recommended approach. This will allow us to evaluate the practical scalability and usefulness of the proposed technology in the real world. It will also allow us to identify any limitations or errors that we may be ignorant of.

## REFERENCES

[1] J. Li, L. Huang, Y. Zhou, S. He, Z. Ming, “Computation partitioning for mobile cloud computing in big data environment,” IEEE Trans. Ind. Informat., vol. 13, no. 4, pp. 2009-2018, Feb. 2017.

[2] K.-K. R. Choo, “Cloud computing: Challenges and future directions,” Trends & Issues in Crime and Criminal Justice, vol. 400, no. 400, pp. 1– 6, Oct. 2010.

[3] M. Pajic, R. Mangharam, O. Sokolsky, D. Arney, J. M. Goldman, and I. Lee, "Model-driven safety analysis of closed-loop medical systems," IEEE Trans. Ind. Informat., vol. 10, no. 1, pp. 3–16, Feb. 2014.

[4] B. Xu, L. D. Xu, H. Cai, C. Xie, J. Hu, and F. Bu, "Ubiquitous data accessing method in IoT-based information system for emergency medical services," IEEE Trans. Ind. Informat., vol. 10, no. 2, pp. 1578– 1586, May. 2014.

[5] G. Yang et al., "A health-IoT platform based on the integration of intelligent packaging, unobtrusive bio-sensor, and intelligent medicine box," IEEE Trans. Ind. Informat., vol. 10, no. 4, pp. 2180–2191, Nov. 2014.

[6] H. Huang, T. Gong, N. Ye, R. Wang, and Y. Dou, "Private and Secured Medical Data Transmission and Analysis for Wireless Sensing Healthcare System," IEEE Trans. Ind. Informat., vol. 13, no.3 pp. 1227-1237, June. 2017.

[7] M. Li, S. Yu, W. Lou, and Y. T. Hou, "Toward privacy-assured cloud data services with flexible search functionalities," in Proc. ICDCSW. IEEE, Macau, CHN, 2012, pp. 466–470.

[8] P. Williams, R. Sion, and B. Carbunar, "Building castles out of mud: practical access pattern privacy and correctness on untrusted storage," in Proc. CCS. ACM, Alexandria, VA, USA, 2008, pp. 139–148.

[9] M. S. Islam, M. Kuzu, and M. Kantarcioglu, "Access pattern disclosure on searchable encryption: Ramification, attack and mitigation," in NDSS, San Diego, CA, USA, 2012.

[10] D. E. Knuth, "Sorting and searching," in The art of computer programming, vol. 3, Boston, USA: Addison-Wesley, 1973.

[11] D. Song, D. Wagner, and A. Perrig, "Practical Techniques for Searches on Encrypted Data," in Proc. of IEEE S&P, DC, USA, 2000, pp. 44-55.

[12] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: improved definitions and efficient constructions," J. Comput.Secur., vol. 19, no. 5, pp. 895-934, 2011.

[13] S. Kamara, C. Papamanthou, and T. Roeder, "Dynamic Searchable Symmetric Encryption," in Proc. of ACM CCS, Raleigh, NC, USA, 2012, pp. 965–976.

[14] S. Kamara, C. Papamanthou, "Parallel and dynamic searchable symmetric encryption," Financial Cryptography and Data Security, Springer Berlin Heidelberg, 2013, pp. 258-274.

[15] G. S. Poh, J.–J. Chin, W.-C. Yau, K.-K. R. Choo, and M. S. Mohamad, "Searchable Symmetric Encryption: Designs and Challenges," ACM Comput. Surv. vol. 50, no. 3, pp. 40:1-40:37, 2017.