International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 05 | May - 2023 Impact Factor: 8.176 ISSN: 2582-3930

A NOVEL APPROACH FOR SECURED HEALTH DATA SHARING OVER THE CLOUD

Dr. Krishna Reddy K R
(Professor, Computer Science Department, S.J.M.I.T., Chitradurga, Karnataka, INDIA krkrishnareddy69@gmail.com)

Mr. Ramesh B E
(Associate Professor, Computer Science Department, S.J.M.I.T.,Chitradurga, Karnataka, INDIAbe.ramesh@gmail.com)

Dr. Aravinda T V
(Professor, Computer Science Department, S.J.M.I.T., Chitradurga, Karnataka, INDIAtvaravinda@gmail.com)

Ms. Chaitrashree A S[1], Ms. Rakshitha M B[2], Ms. Sevanthi U[3], Ms. Syeda Misba Anjum[4]

B.E., 8th Semester,Department of Computer Science and Engineering,

S.J.M.I.T., Chitradurga, Karnataka, INDIA,

chaitrashree57@gmail.com,radhamb18@gmail.com, sevanthiu1910@gmail.com, syedamisbaanjum@gmail.com

Abstract: **-**The security and privacy of patient health records, however, are major issues when it comes to data sharing and outsourcing on the cloud. With the help of developments in virtualization and distributed computing, cloud computing has taken over as the go-to choice for setting up an organization's IT infrastructure. The amount of storage space and remote access needed for medical data is growing. Sharing of patient health records between doctors constitutes the first method. Doctors working in the medical field should exchange similar medical data to enhance patient care and learn on their own. We suggest the similarity test for Cloud-based medical data exchange that protects patient privacy. The second technique, has been used to safely share health records in the cloud. Where the cloud-based secure storage for the collected health record files is located. Similar medical information must be shared by doctors to improve patient autonomy and auxiliary treatment. In this study, an effective data storage and access control system is presented for improving the security and privacy of patient health records.

Keywords: **-***Cloud Computing,CloudStorage, Medical Data Sharing, Distributed Computing, Virtualization, Amazon Web Services(AWS).*

I. INTRODUCTION

Cloud computing has developed as a brand-new technological. Platforms for cloud computing enable clients to manage their infrastructure simply and provide simple access, scalability, stability, reconfiguration, and high performance from their resources over the Internet.

The number of companies and people storing their data on the Cloud is increasing as a result of the new rapidly, expanding paradigm of computing known as "Cloud computing," which provides customers with infinite services, decreasesthe cost of user storage and processing and enhances user simplicity. To store their data, many organizations use cloud services. Instead of depending on healthcare professionals, the user may obtain their medical information via the Cloud. This approach offers secure, user-authenticated, fine-grained data access, and user privacy for medical data[1].

In a private, secure, and confidential setting, a patient's health information is maintained and managed in a personal health record. A patient's sensitive information is intended to give an accurate and thorough overview of a person's medical history that is available online. Most people rarely travel with their medical documents

with them. They do not believe that these medical data will make a significant difference in the event of an emergency, which nobody can anticipate. The program keeps track of previous drugs, history of pharmaceutical allergies, and other pertinent medical or surgical histories[5]. An access request will be sent to the administrator by the doctor if they wish to examine the patient's private information. The doctor must enter this email address in the validate text box. If the doctor is accurate, the doctor will reroute the download page; otherwise, he cannot[7][10]. Due to its accessibility, convenience, and on-demand capabilities, cloud systems may be utilized to provide data-sharing functions[2].

II. RELATED WORK

The proposed architecture includes safeguards to ensure that healthcare and medical information are secure. The cloud allows for the secure exchange of data between healthcare systems[1]. The cloud ensures that data is protected while being transmitted, reducing the risk of outside threats such as man-in-the-middle(MIDM) attacks and data transmission between doctors[2]. Access to a shared file is enabled by password-authenticated users[4].

The approach has the potential to improve the availability of health data while also relieving patients of the burden of maintaining them[6]. Each doctor has a unique id and password to access the hospital firm's cloud database. Doctors can also view patient information. The doctors can only upload the patient's information. By sending a request to an administrator, the doctor can enter using their id and password. The file name will be sent to the doctor through message, and the doctor must see and enter that file name after they log in. If the doctor forgets thepassword, then the new passwordis also sent to the doctor via email[10].

Cloud service providers run the cloud. To keep the owner’s files safe and accessible, it offers paid storage space on its infrastructure accessible to approved users[8][9]. The major goal is to make user interactions with web services simpler and easier. The technology also offers the ability to communicate directly with any doctor [3].

III. PROPOSED METHOD

The figure-1, system design demonstrates how our system was built to function by our project. To connect with the cloud, the user of our system only needs to use the front end of the system. If the credentials the user provided when registering with the system are valid, he or she will be able to connect with the cloud; otherwise, the cloud application will reject the request. According to the service we asked for, the data will be received, and cloud run time will process it and transfer it to storage.

The client side of a cloud computing system is referred to as the front end. It encompasses all of the user interfaces and programs that the client uses to access cloud computing services and resources.

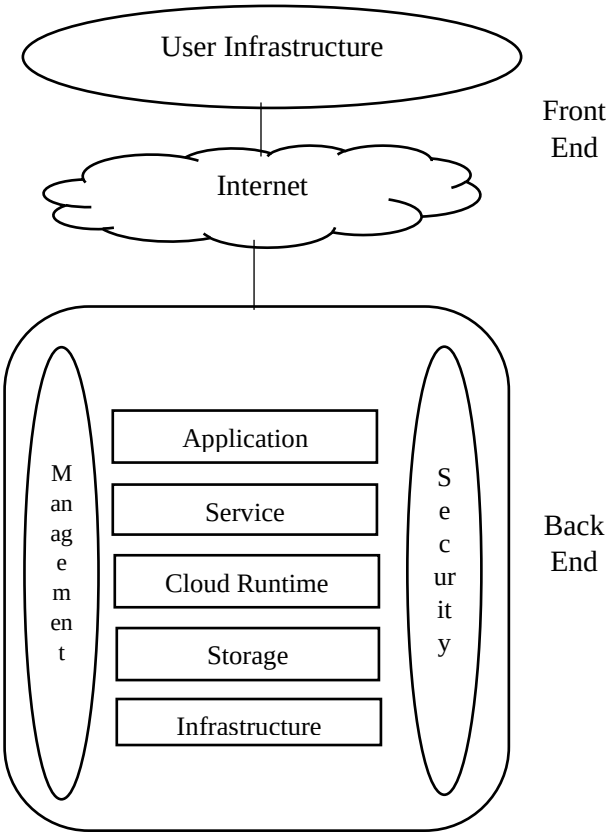

Fig 1: Proposed System Architecture

The cloud that the service provider uses is referred to as the “backend”. It controls the resources, offers security measures, and also holds the resources. Massive storage, virtual

computers, virtual applications, traffic management systems, deployment methodologies, etc. are all included.

The first major advantage of cloud storage is its usefulness and accessibility. Most cloud data storage systems provide an easy-to-use interface and a drag-and-drop feature. Scalable and adaptable cloud storage is offered. You can upgrade the service plan is insufficient.

This data flow diagram i.e., figure 2 refers to the user as the Doctor. Here, the user is divided into two categories: existing users and new users. If the user is already registered, they will input a username and password. If the information is correct, they will be connected to the cloud server. When a new user joins, they must first register. Once the admin doctor has approved and verified their identification, the new user is then linked to the cloud server.

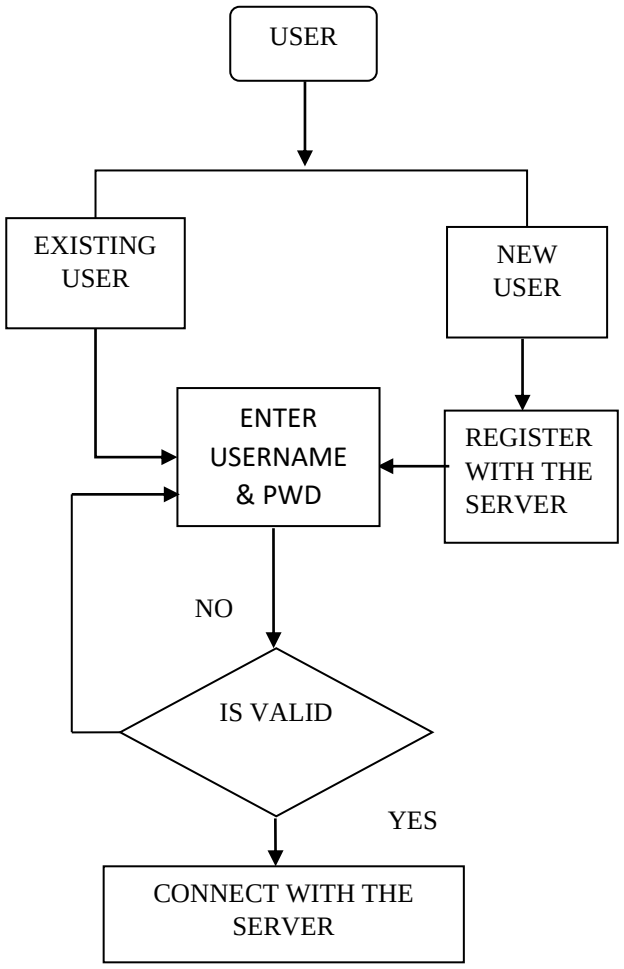

Fig 2: DFD Client

The file sharing from doctor to doctor of patient information via the cloud is shown in Figure 3. While sending the patient records they should first browse the file that they need to be sent.

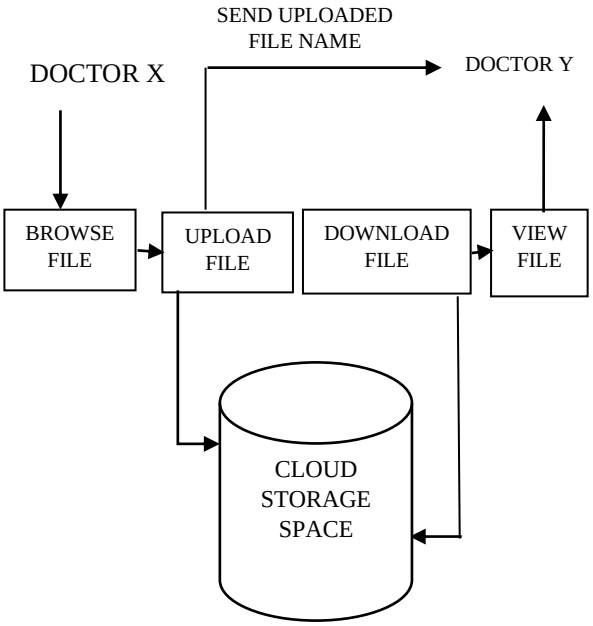

Fig 3: File Sharing System

If another doctor wants to view the patient's sensitive information, the doctor easily downloads the patient's information, the patient information use to understand about patient's condition. In this, the patient information is stored in the cloud database.

MODULES:

I. ADMIN MODULE:

Providing safe patient data is the admin's primary objective. Admin can log in to the software with the proper identification number and password. If their information is true, they may be accepted; otherwise, they will not be permitted. Admins play a crucial role since they are the only ones with complete authority to enter and edit patient information. They also have the right to control the doctor's information. Also, the admin uploads the patient's data.

II. DOCTOR MODULE:

To access the cloud database at the hospital firm, each doctor has a unique ID and password. Also able to see patient information are the physicians. By submitting a request to an admin, the doctor

can log in using their username and password.

III. PATIENT MODULE:

In this module, when the patient's records are read-only, the patient can access their data via the cloud and view their medical records.

IV. CLOUD DATA STORAGE MODULE:

Data is safely stored in this module. The saved data is accessible to and downloadable by authorized users. The owner of the data uploads the patient's medical records to the cloud. Nowadays, having secure access to shared data on a cloud server is essential.

The following are some benefits of the suggested system:

1. Patient information may be kept safe and secure using the system.
2. Patient-specific medical information is difficult to collect or steal.
3. Reduces human interruption and saves time.
4. Patient ID creation is still an additional protection for patient's logins.
5. It simplifies the viewing of patient information by doctors.
6. The application of the technology is safe and adaptable.

ACCOUNT CREATION FOR AMAZON WEB SERVICES:

You'll need to register for an AWS account before you can apply for the AmazonAWS Educate program. The actions listed here.

Step 1: Click Register a Free Account on the aws.amazon.com website.

Step 2: Please enter your Email address. If you already have an Amazon account (one that you use to purchase at amazon.com), you may use it or choose "I am a new user".

Step 3: Click New Account after providing the necessary details.

Step 4: Choose your Account, supply your contact details, and complete the security check. When done, click Create Account and then proceed.

Step 5: Enter your payment details and then press proceed. Your payment card won't be charged until you start using services beyond the Free Tier (if applicable) and any AWS credit codes you've placed into your account. (Take note that some Amazon services cannot be paid for with AWS credits. When visiting the AWS Educate portal, check the FAQs for any limitations.) You can make use of your Higher One account card.

Step 6: For identity verification, provide a phone number, then choose "Call Me Now." The automatic identification verification system used by Amazon must be able to reach you by phone call. On your screen, a PIN will be seen. The mechanism for identification will ask you to enter your PIN.

Step 7: You will be able to proceed with registration when this procedure is finished.

Step 8: Click Proceed after selecting a support plan. The basic(free) level is what most students will use. AWS credits cannot be used to pay for support expenses.

Step 9: The AWS login page will appear once more. Click open the console and log in.

Step 10: Click on your Name in the upper right corner, then select My Account after login in with the newly established account.

Step 11: You will see information about your account. Write down your Account ID. To sign up for AWS Educate, you must have this ID number.

Step 12: Register with AWS Educate.

IV. EXPERIMENT AND RESULTS

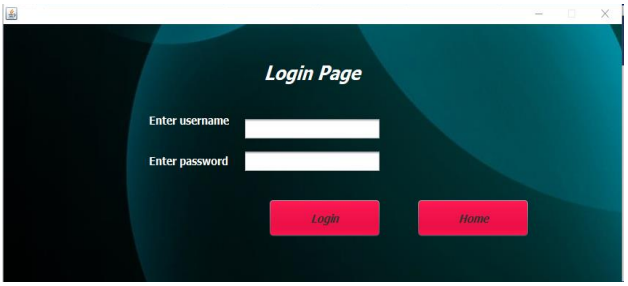

Fig 4: Admin Login Page

Admin login page, where the admin doctor should log in with the username and password to

log in so that they can establish a connection with the cloud.

Fig 5: File Upload Page

Once the connection is established with the cloud, the admin can browse the file they wish to share and can upload it to the cloud, and later can download it.

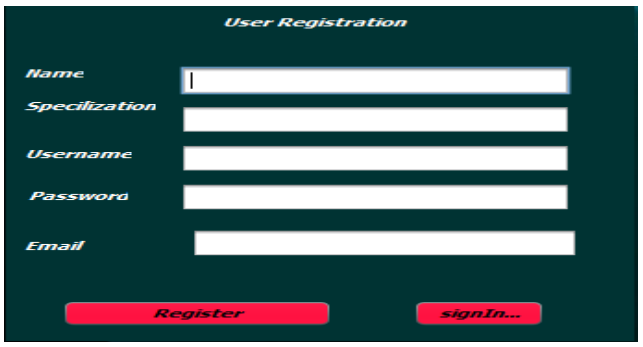

Fig 6: User Registration Page

To log in first, the user should register through their respective name, Email ID, and password.

Fig 7: User Login Page

Doctors must connect with the proper username and password before sharing any data; otherwise, they will not be able to do so. To log in, a new user must first register. If the user forgets his password, they should click the lost password link, and we will send him a new password through email.

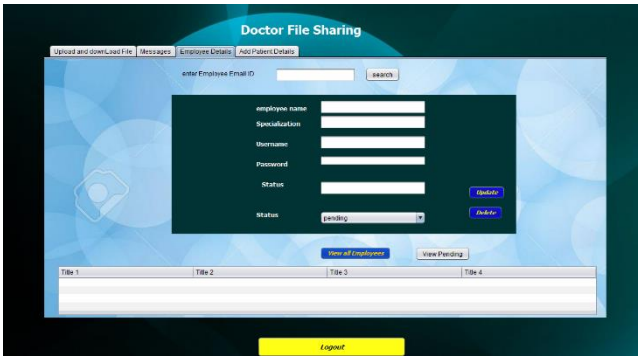

Fig 8: Employee Details Page

Once a user has registered, the admin should check their information before deciding whether to accept them or keep them in pending status. Additionally, the user doctors list and their status can beseen on this page. The pending and accepted doctors can be viewed.

Fig 9: Messages Page

Doctors can examine the messages that have been sent and received by specifying the recipient.

Fig 10: Patient Details Page

After the patient log in, their information is displayed along with a description and any files that the admin or user has uploaded. The patient can view these files and print them if they wish.

V. CONCLUSION

The developed Secure sharing of patient-sensitive information using Cloud Computing. This system is extremely user-friendly. The system is tested with real data. The system is flexible so there is a lot of scope to update the system. The developed system portable has been completed which is customized for the satisfaction of the user. The system has been analyzed, designed, and developed with full care and can be executed without any faults or errors.

Cloud file-sharing is in an upward trend right now, with modern businesses frequently investing in cloud computing and storage infrastructure – and for good reason! Moving your data and workflow to the cloud offers your team the most flexibility when it comes to keeping files and documents consistently backed up and available anywhere, anytime. Doctors use cloud storage to share reports with other Doctors. So that it is easy to download and provides more security for the documents.We presented an effective and versatile distributed system with explicit dynamic data support, including update, delete, and add, to assure the accuracy of doctor's data in cloud data storage

REFERENCES

1. G. Revathy, P. Muruga Priya, R. Saranaya and C. Ramachandran, "Cloud Storage and Authenticated Access For Intelligent Medical System," *2022 6th International Conference on Computing Methodologies and Communication (ICCMC)*, Erode, India, 2022, pp.53-56, doi: 10.1109/ICCMC53470.2022.9753765.
2. N. Santos, W. Younis, B. Ghita, and G. Masala, "Enhancing Medical Data Security on Public Cloud," 2021 IEEE International Conference on Cyber Security and Resistance (CSR), Rhodes, Greece, 2021, pp. 103-108, doi:10.1109/CSR51186 2021.9527987.
3. S. Swathi, E. Saranya, R. M. Prabakaran, M. Sachin Kumar and S. Bairavel, "Virtual Health Assistant,"*2021 International Conference on System, Computation, Automation and Networking (ICSCAN)*, Puducherry, India, 2021, pp. 1-4, doi: 10.1109/ICSCAN53069.2021.9526460.
4. O. A. Khashan, "Secure Outsourcing and Sharing of Cloud Data Using a User-Side Encrypted File System," in *IEEE Access*, vol. 8, pp. 210855-210867, 2020, doi: 10.1109/ACCESS.2020.3039163.
5. S. Xie, F. Wu, X. Zhang, W. Yao, and Z. Zheng, "Similarity Test for Privacy-Preserving Medical Data Sharing Based on NTRU Encryption," *2019 IEEE 9th International Conference on Electronics Information and Emergency Communication (ICEIEC)*, Beijing, China, 2019, pp. 1-4, doi: 10.1109/ICEIEC.2019.8784488.
6. H. S. G. Pussewalage and V. Oleshchuk, "A Patient-Centric Attribute Based Access Control Scheme for Secure Sharing of Personal Health Records Using Cloud Computing," *2016 IEEE 2nd International Conference on Collaboration and Internet Computing (CIC)*, Pittsburgh, PA, USA, 2016, pp. 46-53, doi: 10.1109/CIC.2016.020.
7. P. Solapurkar, "Secure sharing of personal health records on the cloud using key-aggregate cryptosystem," *2015 International Conference on Information Processing (ICIP)*, Pune, India, 2015, pp. 278-283, doi: 10.1109/INFOP.2015.7489393.
8. M. Malarvizhi, J. A. J. Sujana, and T. Revathi, "Secure file sharing using cryptographic techniques in the cloud," *2014 International Conference on Green Computing Communication and Electrical Engineering (ICGCCEE)*, Coimbatore, India, 2014, pp. 1-6, doi: 10.1109/ICGCCEE.2014.6921421.
9. S. Zhu, X. Yang, and X. Wu, "Secure Cloud File System with Attribute-Based Encryption," *2013 5th International Conference on Intelligent Networking and Collaborative Systems*, Xi'an, China, 2013, pp. 99-102, doi: 10.1109/INCoS.2013.22.
10. Kiruthika. G, Bala Sugitha. G, 2016, "Secure Sharing of Patient's Sensitive Information using Cloud Computing," *International Journal Of Engineering Research & Technology (Ijert) Ncicct – 2016* (Volume 4 – Issue 19).