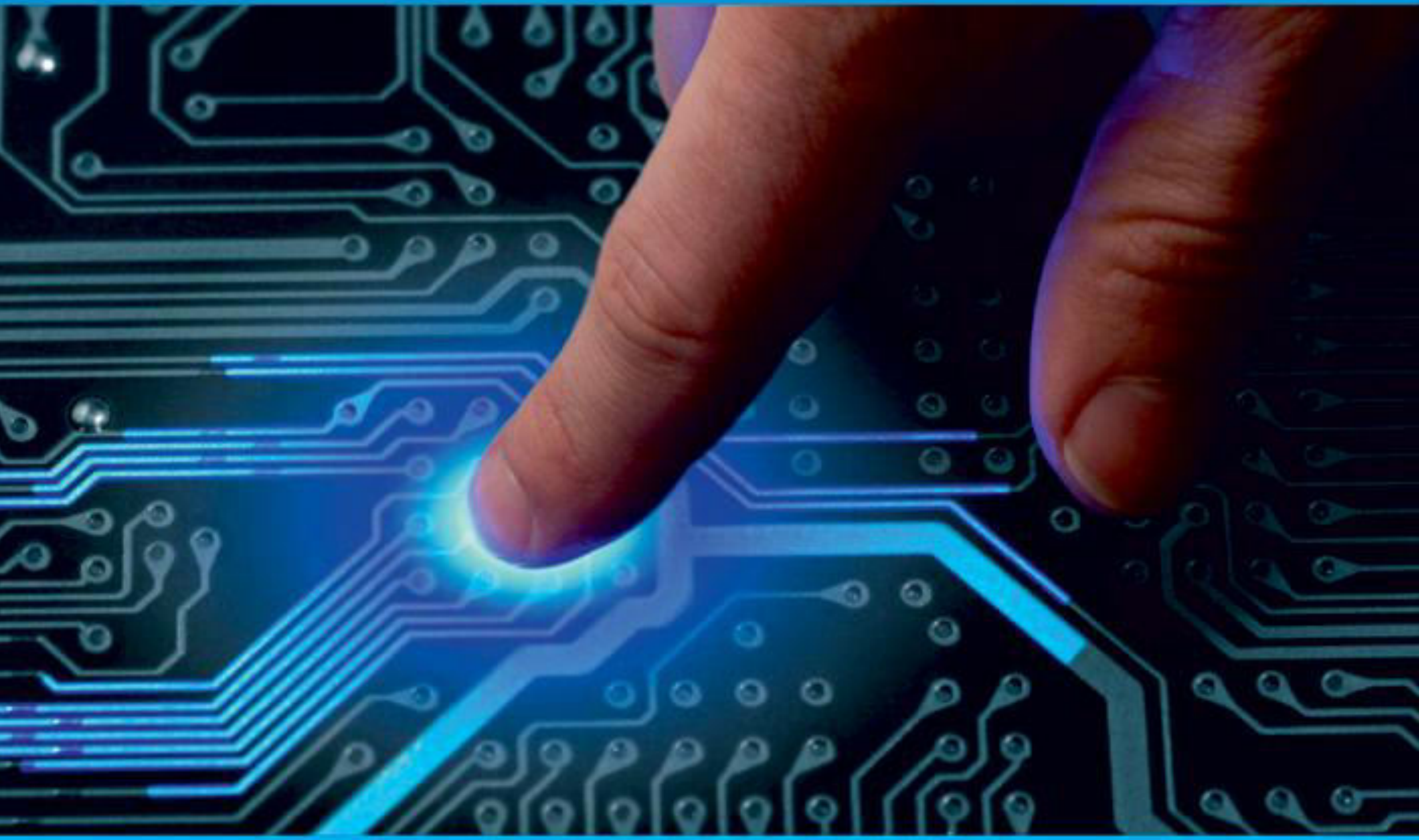
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 1, January 2023

ISSN
INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.165

9940 572 462 6381 907 438 ijircce@gmail.com www.ijircce.com

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 11, Issue 1, January 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1101010 |

Mechanism for Data Sharing and Secure Keyword Search in Cloud Computing

C.Sai Himaja, K.Arjun

PG Student, Dept. of C.S.E., Bheema Institute of Technology & Science, Adoni, India

Asst. Professor, Dept. of C.S.E., Bheema Institute of Technology & Science, Adoni, India

ABSTRACT: The cost of resources for hardware and software in computer infrastructure has drastically decreased with the rise of cloud infrastructure. Before being sent to the cloud, the data is often encrypted to protect security. It is difficult to look for and distribute data that has been encrypted, as contrast to plain data. However, it is a crucial responsibility for the cloud service provider since customers depend on the cloud to quickly search for their data and deliver the results without jeopardising the confidentiality of their data. We suggest a cypher text-policy attribute-based approach with keyword search and data sharing (CPAB-KSDS) for encrypted cloud data to get around these issues. Contrary to existing systems, which only offer one of two aspects, the suggested approach not only permits attribute-based data exchange but also provides attribute-based keyword search. Furthermore, our technique allows for the updating of the keyword without interacting with the PKG during the sharing phase. In this study, the concept of CPAB-KSDS and its security model are discussed. Additionally, we provide a specific technique and demonstrate that it is safe in the random oracle model and resistant to selected ciphertext and chosen keyword attacks. Finally, the efficiency and property comparison shows how feasible and effective the suggested building is.

KEYWORDS: Searchable Attribute-based Encryption, Cloud Data Sharing, Attribute-based Proxy Re-encryption, Keyword Update.

I. INTRODUCTION

The lack of optimal use of the people as well as material resources available for providing integrated healthcare to prevent illnesses and cure them after they have occurred is a frequent occurrence in the majority of Arab nations. According to statistics, health issues including diabetes, liver disease, and parasitic illnesses like malaria and histoplasmosis are prevalent in significant numbers in Arab nations. Early diagnosis of certain health issues might stop their complications or stop them before they start. This is because of a number of planning, operational, and technical concerns. If we could get beyond them, the standard of healthcare would advance significantly. Hospital information systems, some of the most cutting-edge software that directly supports all administrative and technical healthcare activities, are also a weakness and a resource shortage. These systems guarantee that the medical institution has complete control over all of its operations and resources. The precise choice of hardware and storage software does not determine how well these sophisticated systems perform. Rather, their success depends on their compatibility for many users, including healthcare practitioners like physicians, nurses, technicians, and even administrators, whose information demands, as well as the visions and objectives of each of these groups, differ from one another.

Due to a variety of problems, including limited store capacity, high operating and maintenance expenses, and poor system integration, the old health system (paper) has been replaced with an electronic health information system. Cloud computing then took the role of the computerised health system since it is based on a more effective infrastructure and offers numerous advantages over traditional IT solutions, including cost, scalability, flexibility, and other aspects [2]. The use of the cloud in healthcare will be encouraged by the fact that the utilization of cloud computing with electronic health records lowers costs associated with the delivery of healthcare services, network maintenance, licencing fees, and infrastructure in generally [2], [3].

Concerns concerning critical privacy and data security issues have been highlighted by the quick move to the cloud and its application in healthcare systems [4], [5]. Healthcare professionals' attention is diverted away from infrastructure administration and toward clinical and patient-related services as a result of the adoption of the cloud in IT [6]. A variety of difficulties with privacy, security, access, and compliance have arisen as a result of the sharing of personal and medical information via the Internet and on numerous servers outside of the secure environment of the healthcare institution [7], [8], [9], [10].

There are currently no effective frameworks in the literature that explicitly cover all workable plans and connections among cloud computing and biomedical technology [11], [12]. Several scholars have looked into how to improve the healthcare framework for cloud computing [13], [14], and [15]. The usage of cloud healthcare will grow, and healthcare providers will be encouraged to utilize cloud-based services as more research and answers to these problems are made available [16].

The following is a summary of our contributions: creates a framework for governmental healthcare services that is adaptable, safe, affordable, and protects privacy by: o Using the most modern encryption and decryption techniques that are appropriate for cloud-based EHR systems and applying, updating, and using them. The suggested plan avoids using the conventional encryption method since it is inappropriate for the cloud environment. o Achieving the capacity to govern and grow computer resources in accordance with the necessary health services. The EHR can accommodate large-scale data transfers. · Providing a practical way for government health sector decision-makers to implement cloud-based healthcare solutions, particularly in developing nations.

II. LITERATURE REVIEW

A Review of Cloud Computing Technology Solution for Healthcare System

Prior to its replacement by the Health Care Information System, the old paper-based healthcare information system was in use in the healthcare industry (HIS). However, it was discovered that the HIS did not operate efficiently because to a number of problems including storage capacity, systems engineering, high running costs, and system maintenance. A new technology called cloud computing makes it possible to access software, infrastructure, and a computer platform as a service anywhere, at any time, through the Internet. Many issues with the healthcare system have been stated to be resolved by this technology, including adding new capabilities and expanding storage capacity. Cloud computing is more affordable, improves accessibility and interoperability, makes resources more efficient, and integrates healthcare information systems. It serves as a remedy for the present problems, enhancing the features and performance of the healthcare information systems. The purpose of this project is to investigate cloud computing as a potential remedy for problems with the healthcare information system. Data transmission, storage, pricing, and maintenance challenges, among others, are discussed and presented. After then, the study's ramifications were explored.

Cloud Computing in Healthcare: A Space of Opportunities and Challenges

It is imperative that healthcare businesses think about implementing health information technology (HIT) systems as the price of healthcare services rises and healthcare personnel become more and more difficult to come by. HIT enables health organisations to simplify a number of their procedures and deliver services more effectively and economically. Modern technical developments like Cloud Computing (CC) offer a solid platform and a real facilitator for HIT services delivered via the Internet. This may be done via the "e-Health Cloudpay-per-use "'s approach, which will allow the healthcare sector meet present and future demand while keeping expenses to a minimum. Despite having enormous promise, the literature hasn't focused much on HIT as a CC model. There don't seem to be any frameworks that completely include all workable plans and connections among HIT and CC. It is crucial to evaluate and compare the efficacy of such systems. This article introduces the idea of "e-Health Cloud," highlighting many of its components, suggesting the creation of an e-health environment, and outlining many of the obstacles that stand in the way of the e-Health Cloud's success. We will also talk about several options for dealing with issues like security and privacy.

A KP-ABPRE with keyword search technique was created to enable a server to both search for and re-encrypt a certain ciphertext [36]. In contrast to a standard key policy ABE system, the data owner in this scheme has no influence over the access policy that is applied to his encrypted data. Though it is important to note that in a PHR system [11], [12], each data owner should have complete control over the shared data. As a result, a ciphertext policy attribute-based encryption method that includes keyword searching and data exchange is preferred. Another problem with the work [36] is the fact that data owner must communicate with the PKG in order to ask it to produce a search token, significantly increasing the PKG's workload. In addition, the data that must be shared with the delegatee that is unrelated to the PKG must be shared by the delegator. The creation of an attribute-based encryption method facilitating data finding and sharing without the use of PKG during in the searching and transferring phase is therefore left as an open challenge.

III. PROPOSED WORK

Prior work failed to show that attribute-based procedures could allow data sharing and keyword search in the same framework without turning to PKG. Therefore, a novel attribute-based technique is required to fulfil the objective for the PHR situation described above. One may claim that by combining an AB-PRE method and an attribute-based keyword search strategy, the issue can be easily overcome (AB-KS). However, the combination might lead to two significant problems: 1) The combined method is not CCA secure, and 2) a collusion attack might exploit it. In order to properly enable keyword searching, data exchange, and the protection of keyword privacy, a secure system is necessary. These worries encourage us to create a device that:

1) Allows the data owner to search and share the encrypted health report without the unnecessary decryption process.
2) Supports keyword updating during the data sharing phase.
3) More importantly, does not need the exist of the PKG, either in the phase of data sharing or keyword updating.
4) The data owner can fully decide who could access the data he encrypted.

For encrypted cloud data, we first provide a ciphertext-policy attribute-based approach with search query and data sharing (CPAB-KSDS). The ciphertext-policy option has the sharing and searching features turned on. Additionally, our system allows the keyword to be modified as the file is being shared. After outlining the design of our mechanism, we demonstrate the random oracle model's resistance to the selected ciphertext attack (CCA) and the chosen keyword attack (CKA). The performance and property comparison shows how feasible and effective the planned building is.

1. Architecture:

Five entities make up the CPAB-KSDS system, which is depicted in Figure 1: the PKG, the cloud server (which serves as a proxy), the owner of the health record, the delegator (who receives the original ciphertext), and the delegatee (recipient of the re-encrypted ciphertext). The following is a description of the system's process.

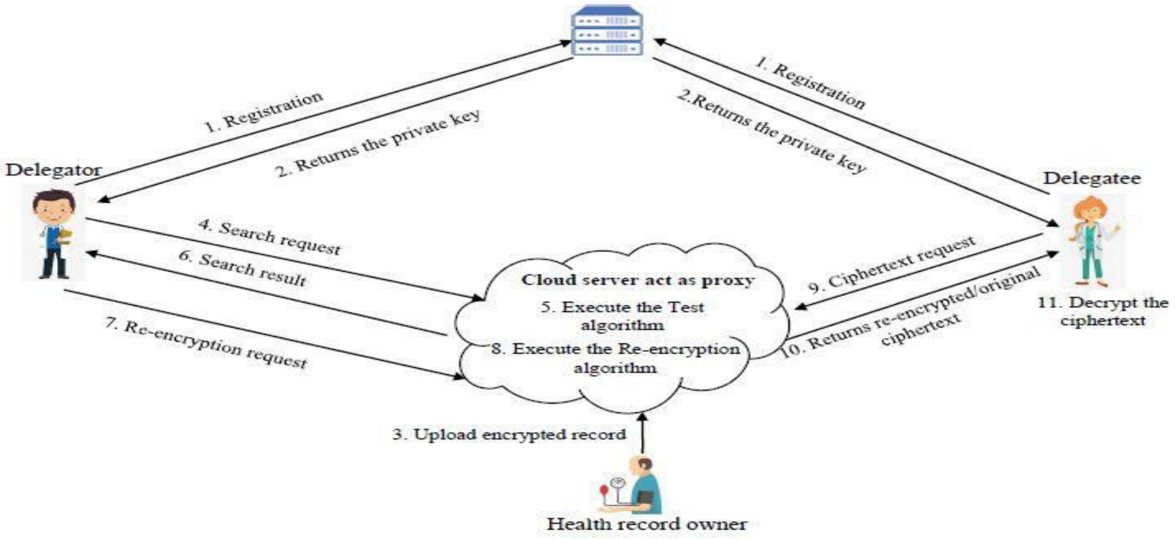

1. Registration
2. Returns the private key
1. Registration
2.Returns the private key
Delegator
Delegatee
4. Search request
6. Search result
7. Re-encryption request
Cloud server act as proxy
5. Execute the Test algorithm
8. Execute the Re-encryption algorithm
9. Ciphertext request
10. Returns re-encrypted/original ciphertext
11. Decrypt the ciphertext
3. Upload encrypted record
Health record owner

Fig 1: System Architecture

1. **System Initialization**
2. **Registration**
3. **Ciphertext Upload**
4. **Ciphertext Search**

5. **Re-encryption**
6. **Decryption**

1. System Initialization

System Initialization: This phase is executed by the PKG. The PKG generates the system public parameters that are publicly available for all the participants of the system and the master secret key which is kept private by the PKG.

2. Registration

Registration: The registration phase is executed by the PKG. When each user issues a registration request to the PKG, the PKG generates a private corresponds to his attribute set.

3. Ciphertext.

Ciphertext Upload: The personal health record owner encrypts his record with the original recipient's policy and the keyword, and then upload the encrypted record to the cloud server.

4. Ciphertext Search:

The recipient generates a search token and issues a search request contains the search token to the cloud server. The cloud server searches the ciphertext via the Test algorithm and returns the search result to the recipient.

5. Re-encryption:

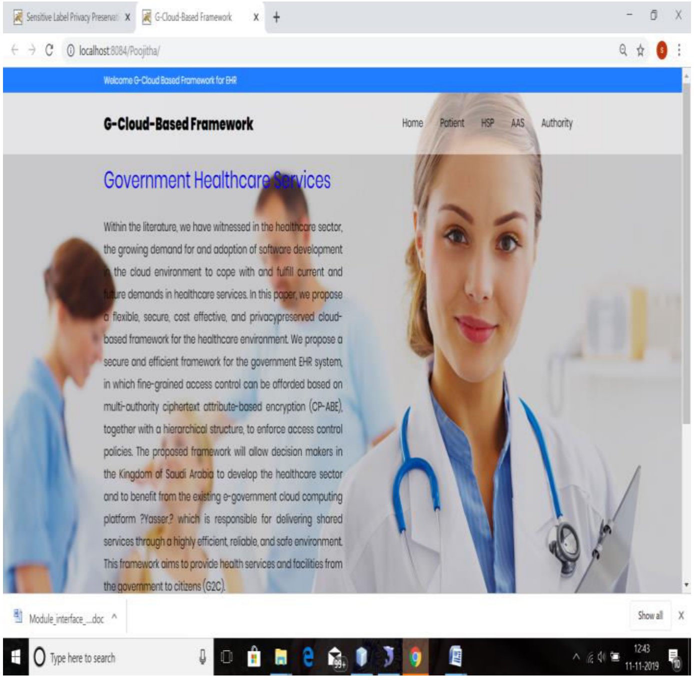
The delegator generates a re-encryption key and issues a re-encryption request contains the re-encryption key to the cloud server. The cloud server converts the original encrypted record to a re-encrypted ciphertext under a new access policy.

6. Decryption:

The recipient (a delegatee or a delegator) requests a re-encrypted (or an original) ciphertext from the cloud server and then decrypts the ciphertext with his own private key to get the underlying record. Note that, a delegatee may act as a delegator for other participants.

Output:

Home Page



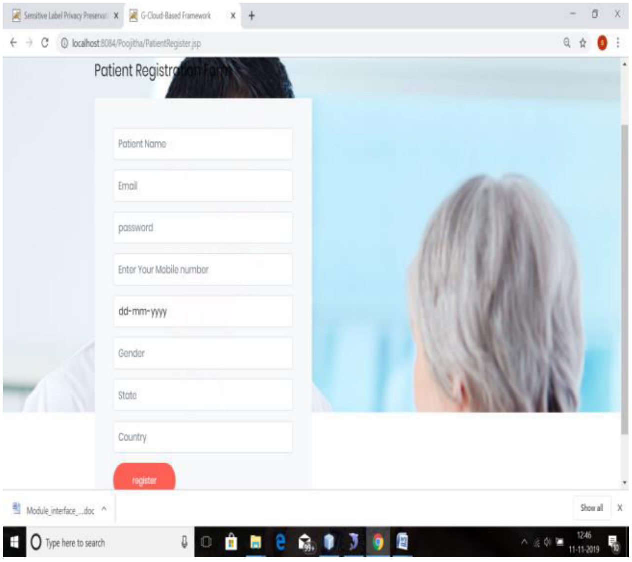
Welcome G-Cloud Based Framework for EHR

G-Cloud-Based Framework

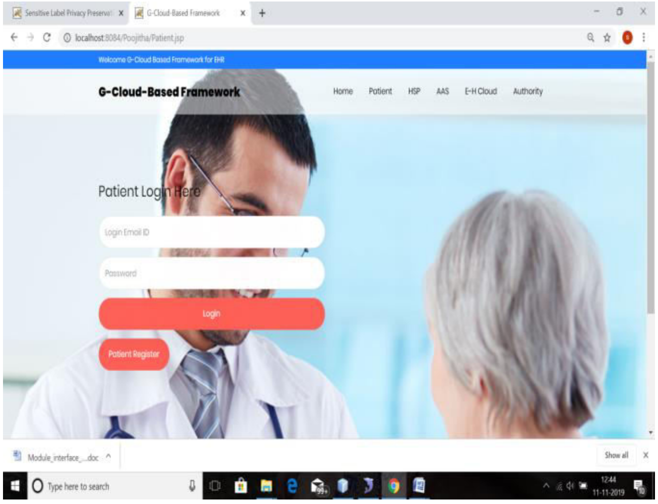
Government Healthcare Services

Within the literature, we have witnessed in the healthcare sector, the growing demand for and adoption of software development in the cloud environment to cope with and fulfill current and future demands in healthcare services. In this paper, we propose a flexible, secure, cost effective, and privacypreserved cloud-based framework for the healthcare environment. We propose a secure and efficient framework for the government EHR system, in which fine-grained access control can be afforded based on multi-authority ciphertext attribute-based encryption (CP-ABE), together with a hierarchical structure, to enforce access control policies. The proposed framework will allow decision makers in the Kingdom of Saudi Arabia to develop the healthcare sector and to benefit from the existing e-government cloud computing platform ?Yasser,? which is responsible for delivering shared services through a highly efficient, reliable, and safe environment. This framework aims to provide health services and facilities from the government to citizens (G2C).

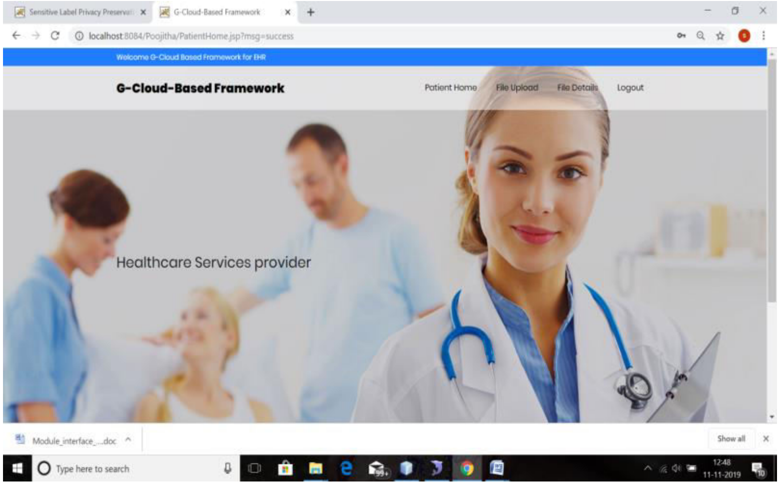
Patient Registration Form



Patient Login Form

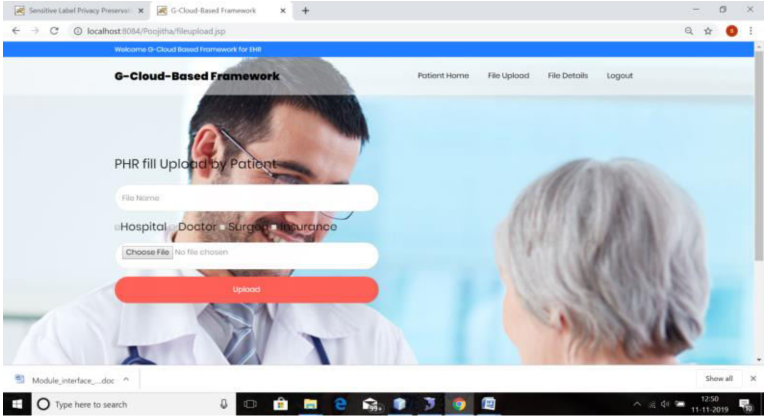


Patient Home Page



Healthcare Services provider

Patient Upload File



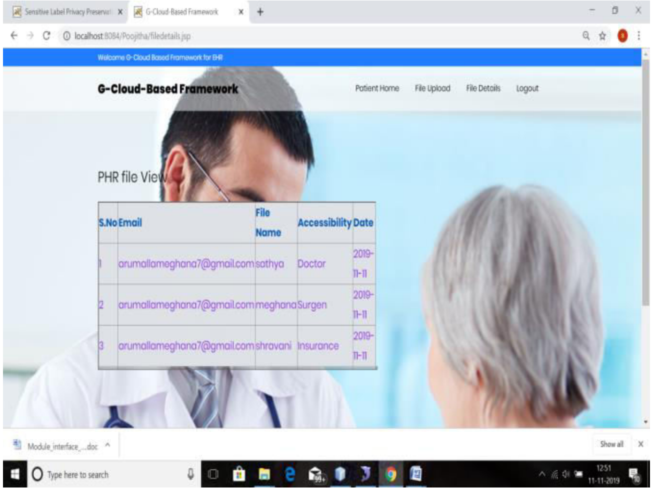
PHR fill Upload by Patient

File Name

□ Hospital □ Doctor □ Surgen □ Insurance

Choose File No file chosen

Patient Upload File Details



PHR file View

S.No	Email	File Name	Accessibility	Date
1	arumallameghana7@gmail.com	sathya	Doctor	2019-11-11
2	arumallameghana7@gmail.com	meghana	Surgen	2019-11-11
3	arumallameghana7@gmail.com	shravani	Insurance	2019-11-11

IV. CONCLUSION

This study introduces a novel idea of ciphertext-policy attribute-based mechanism (CPAB-KSDS) to allow data sharing and keyword searches. In this study, a real CPAB-KSDS scheme is built, and its CCA security in the random oracle model is demonstrated. By comparing performance and property, the suggested plan is shown to be effective and workable. The challenge of creating attribute-based encryption with keyword searching as well as data sharing even without PKG during the sharing phase is addressed in this research with a positive response to the open, hard topic raised in the past work [36]. Additionally, our work inspires intriguing unsolved issues, such as developing a CPAB-KSDS scheme without random oracles or suggesting a new framework to facilitate more expressive keyword search.

REFERENCES

[1] Masrom, Maslin, and Ailar Rahimli. "A Review of Cloud Computing Technology Solution for Healthcare System." Research Journal of Applied Sciences, Engineering and Technology 8, no. 20 (2014): 2150–2155.

[2] HUCÍKOVÁ, Anežka, and Ankica Babic. "Cloud Computing in Healthcare: A Space of Opportunities and Challenges." Transforming Healthcare with the Internet of Things (2016): 122.

[3] Yang, Haibo, and Mary Tate. "A descriptive literature review and classification of cloud computing research." CAIS 31 (2012): 2.

[4] Zissis, Dimitrios, and Dimitrios Lekkas. "Addressing cloud computing security issues." Future Generation computer systems 28, no. 3 (2012): 583–592.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

☎ 9940 572 462 6381 907 438 ijircce@gmail.com

Scan to save the contact details

www.ijircce.com