G-CLOUD: SECURE FRAMEWORK FOR GOVERNMENT HEALTH CARE

SAYYAD ARIFA [#1], K.VENKATESH [#2]

[#1] MCA Student, Master of Computer Applications,

D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.

[#2] Assistant Professor, Master of Computer Applications,

D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.

Abstract

Now a days cloud computing is increasing its attention towards data storage and accessing from several users range from small scale companies to large scale companies.As we have witnessed in the healthcare sector, there is a great demand for cloud in order to store and access the documents for end users.But current cloud servers in government health care services are not providing complete security and flexibility. In this project, we propose a flexible, secure, cost effective, and privacy- preserved cloud-based framework for the healthcare environment. We propose a secure and efficient framework for the government EHR system, in access control can be afforded based on multi-authority attribute-based encryption (MABE), together with a hierarchical structure, to enforce access control policies.

1. INTRODUCTION

A common phenomenon in healthcare in most Arab countries is the lack of optimal utilization of human and material resources available to provide integrated healthcare to prevent diseases and treat diseases after they occur. Statistics indicate that Arab countries suffer from high rates of health problems, such as diabetes, liver disease, and parasitic diseases, such as histosomiasis and malaria. These health problems could be prevented before they occur or their complications prevented by early detection. This is due to a combination of factors: planning, operational, and technical. If we were able to overcome them, this would lead to significant progress in the level of health care. In addition, there is a weakness and lack of available hospital information systems, which is some of the most advanced software that directly serves all technical and administrative healthcare

activities, ensuring that the medical institution has full control over all its activities and resources. The successes of these advanced systems do not depend on the exact selection of equipment and software for storage. Rather, their success   depends on their suitability for different users—from healthcare providers, such as doctors, nurses, technicians, and even administrators—where the vision and priorities of each of these categories differ, and their information needs vary, as do the benefits of each of these systems.

PROJECT PURPOSE

The traditional health system (paper) has been replaced by an electronic health information system because the traditional system has been found to be ineffective due to a number of issues, including low storage capacity, high operating and maintenance costs, and system integration [1]. The computerized health system was then replaced by cloud computing because it relies on a more efficient infrastructure, as well as the many benefits of cloud computing in IT, such as cost, scalability, flexibility, and other features [2]. The use of cloud computing in electronic health records reduces costs in the provision of health services, maintenance costs, networks, licensing fees, and infrastructure in general, and this will therefore encourage developers to adopt the cloud in healthcare [2], [3].

The rapid shift to the cloud and its use in healthcare systems has raised concerns about crucial issues of privacy and information security [4], [5]. The adoption of the cloud in IT increases the focus and concern of healthcare providers on clinical and patient-related services and reduces attention on infrastructure management [6]. The sharing of personal and health information across the Internet and various servers outside the safe environment of the healthcare institution has led to a number of problems related to privacy, security, access, and compliance issues [7], [8], [9], [10]. In the literature, there are no existing powerful frameworks that clearly address all viable schemes and interrelationships between cloud computing and healthcare technology [11], [12]. Improving the framework for healthcare in cloud computing has been studied by several researchers [13], [14], [15]. Further developments and solutions in these challenges will increase the adoption of cloud healthcare and encourage healthcare providers to move forward with cloud-based services [16].The traditional health system (paper) has been replaced by an electronic health information system because the traditional system has been found to be ineffective due to a number of issues, including low storage capacity, high operating and maintenance costs, and system integration [1]. The computerized health system was then replaced by cloud computing because it relies on a more efficient infrastructure, as well as the many benefits of cloud computing in IT, such as cost, scalability, flexibility, and other features [2]. The use of cloud computing in electronic health records reduces costs in the provision of health services, maintenance costs, networks, licensing fees, and infrastructure in general, and this will therefore encourage developers to adopt the cloud in healthcare [2], [3].

PROJECT OVERVIEW

The sharing of personal and health information across the Internet and various servers outside the safe environment of the healthcare institution has led to a number of problems related to privacy, security, access, and compliance issues [7], [8], [9], [10]. In the literature, there are no existing powerful frameworks that clearly address all viable schemes and interrelationships between cloud computing and healthcare technology [11], [12]. Improving the framework for healthcare in cloud computing has been studied by several researchers [13], [14], [15]. Further developments and solutions in these challenges will increase the adoption of cloud healthcare and encourage healthcare providers to move forward with cloud-based services [16].

2 .LITERATURE SURVEY

INRODUCTION

Literature survey is the most important step in software development process. Before developing the tool, it is necessary to determine the time factor, economy and company strength. Once these things are satisfied, ten next steps are to determine which operating system and language used for developing the tool. Once the programmers start building the tool, the programmers need lot of external support. This support obtained from senior programmers, from book or from websites. Before building the system the above consideration r taken into for developing the proposed system.

RELATED WORK

Masrom, Maslin, and Ailar Rahimli.   [1]: proposed A Review of Cloud Computing Technology Solution for Healthcare System Previously the traditional healthcare information system that used in the healthcare sector was the paperbased and then later it was replaced by the Healthcare Information System (HIS). However the HIS was found not perform effectively because of several issues such as storage capacity, system integration, high operating cost and system maintenance. Cloud computing is a new technology that deliver the software, infrastructure and computational platform as a service over the Internet in any place and any time. This technology has been said can solve many problems of the healthcare system such as increase the storage capacity and add new capability on the existing healthcare system. Cloud computing offers cost effective, increase interoperability and accessibility, optimize resources and integrate the healthcare information systems. It becomes a solution for solving the current issues, which lead to enhance functionality and features of the healthcare information systems. Therefore, the aim of this study is to explore the cloud computing technology as solution for healthcare information system issues. Issues such as data transmission, data storage, cost and maintenance issues are presented and described. The implications of this study then discussed.

Anežka Hucíková [2]: stated that Cloud computing is a model of self-service on-demand network access enabling delivering computing resources and services. Contemporary research shows that around 50% of healthcare companies from large hospitals to ambulatory services across the US and Europe have already deployed cloud technology. Since the technology is simultaneously evolving, more healthcare companies are expected to move their enterprise communication to the cloud. There is a need for a more complex understanding of opportunities and challenges for technology providers and healthcare organizations. Secondary, the poster aims to suggest how such specific challenges can be dealt with.

Yang, Haibo, and Mary Tate et.al [3]: discussed about the cloud as we present a descriptive literature review and classification scheme for cloud computing research. This includes 205 refereed journal articles published since the inception of cloud computing research. The articles are classified based on a scheme that consists of four main categories: technological issues, business issues, domains and applications, and conceptualising cloud computing. The results show that although current research is still skewed towards technological issues, new research themes regarding social and organisational implications are emerging. This review provides a reference source and classification scheme for IS researchers interested in cloud computing, and to indicate under-researched areas as well as future directions.

Dimitrios Lekkas **et.al [4]:** discussed about The recent emergence of cloud computing has drastically altered everyone's perception of infrastructure architectures, software delivery and development models. Projecting as an evolutionary step, following the transition from mainframe computers to client/server deployment models, cloud computing encompasses elements from grid computing, utility computing and autonomic computing, into an innovative deployment architecture. This rapid transition towards the clouds, has fuelled concerns on a critical issue for the success of information systems, communication and information security. From a security perspective, a number of unchartered risks and challenges have been introduced from this relocation to the clouds, deteriorating much of the effectiveness of traditional protection mechanisms. As a result the aim of this paper is twofold; firstly to evaluate cloud security by identifying unique security requirements and secondly to attempt to present a viable solution that eliminates these potential threats. This paper proposes introducing a Trusted Third Party, tasked with assuring specific security characteristics within a cloud environment. The proposed solution calls upon cryptography, specifically Public Key Infrastructure operating in concert with SSO and LDAP, to ensure the authentication, integrity and confidentiality of involved data and communications. The solution, presents a horizontal level of service, available to all implicated entities, that realizes a security mesh, within which essential trust is maintained.

3. EXISTING SYSTEM

All the existing medical data sharing organizations used to store their valuable and sensitive information inside the cloud server in a plain text manner. So there is no security for the sensitive data which is stored inside the cloud server.

LIMITATIONS

1. All the primitive cloud servers or cloudlets laid a way for the intruder to crack the information illegally from the cloud server.

2. And there is no concept like de-centralized data access in the primitive clouds which is one of the main limitation in the existing clouds.

3. There is no facility like Secret-authority (SA) in order to grant keys for downloading the files in secure manner by the government health users.

4. PROPOSED SYSTEM

In this project, we propose a flexible, secure, cost effective, and privacy- preserved cloud-based framework for the healthcare environment. We propose a secure and efficient framework for the government EHR system, in access control can be afforded based on multi-authority attribute-based encryption (MABE), together with a hierarchical structure, to enforce access control policies.

ADVANTAGES OF THE PROPOSED SYSTEM

The following are the advantages of the proposed system. They are as follows:

1. It is an efficient authenticated structure.

2. It is the first practical mechanism which provided security against the intruders for the sensitive information.

The theoretical and experimental results show that our proposed application is more efficient,

5. SOFTWARE PROJECT MODULES

Implementation is the stage where the theoretical design is converted into programmatically manner. In this stage we will divide the application into a number of modules and then coded for deployment. We have implemented the proposed concept on Java programming language with JSE as the chosen language in order to show the performance this proposed protocol. The application is divided mainly into following 4 modules. They are as follows:

1. Health Care providers (HCP) Module

2. Data User/patients Module

3. E-Cloud Service Module

4. Trusted Key Authority Module

Now let us discuss about each and every module in detail as follows:

5.1 HEALTH CARE PROVIDER MODULE

In this module, the data owner /HCSP try to uploads their data in the cloud server. For the security purpose the data owner encrypts the patients details and will do the following operations like Upload Patient Details, View All My Uploaded Patients, View Public Keys, View Transaction Details.

5.2 PATIENTS/USER MODULE

In this module, user logs in by using his/her user name and password. After Login user requests search control to cloud and will Search for Patients based on the index keyword with the Score of the searched Patient and downloads the Patient. User can view the search of the Patients and also do some operations like Search, Request Key, Request File, and View Keys

5.3 E-CLOUD SERVER MODULE

The cloud server manages a cloud to provide data storage service. Data owners encrypt their data Patients and store them in the cloud for sharing with Remote User and will do the following operations like View HSPs and Patients, View Patient Details, View Attackers,View Patient Keys,Un Revoke User ,View Transaction ,View Transactions Results ,View Time Delay Results ,View Throughput Results
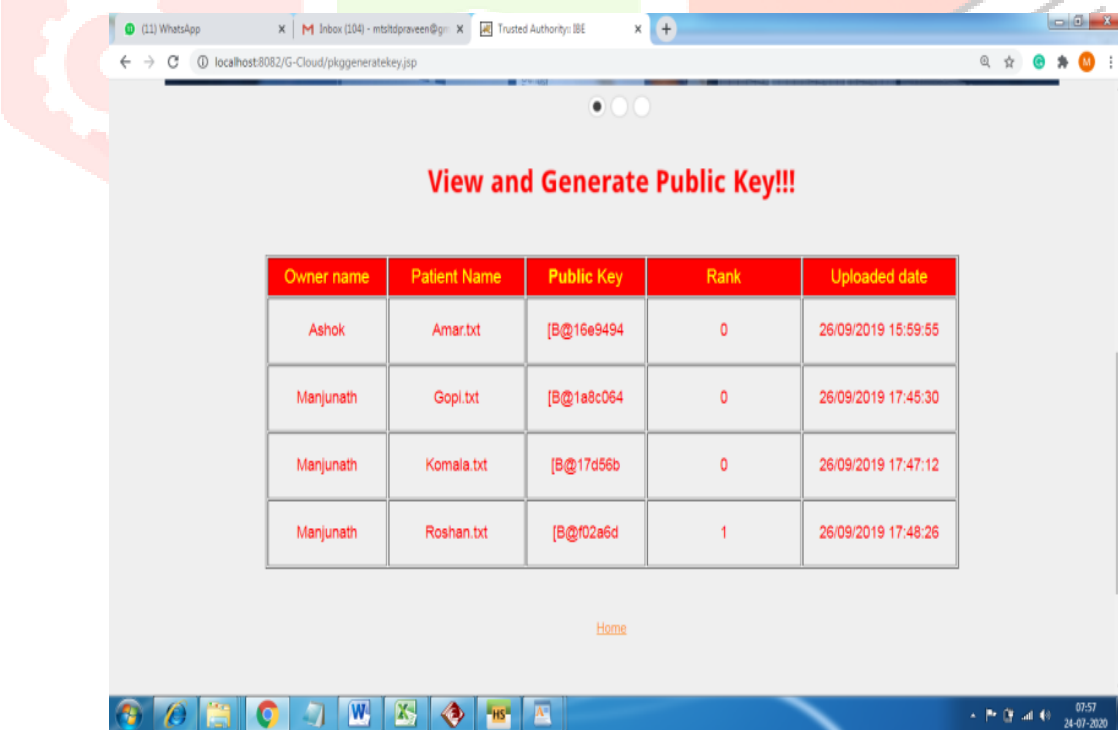
5.4 TRUSTED KEY AUTHORITY MODULE

In this module, TA logs in by using his/her user name and password. After Login he will do some operations like View all Patients, Generate Public Key Requests, key generation
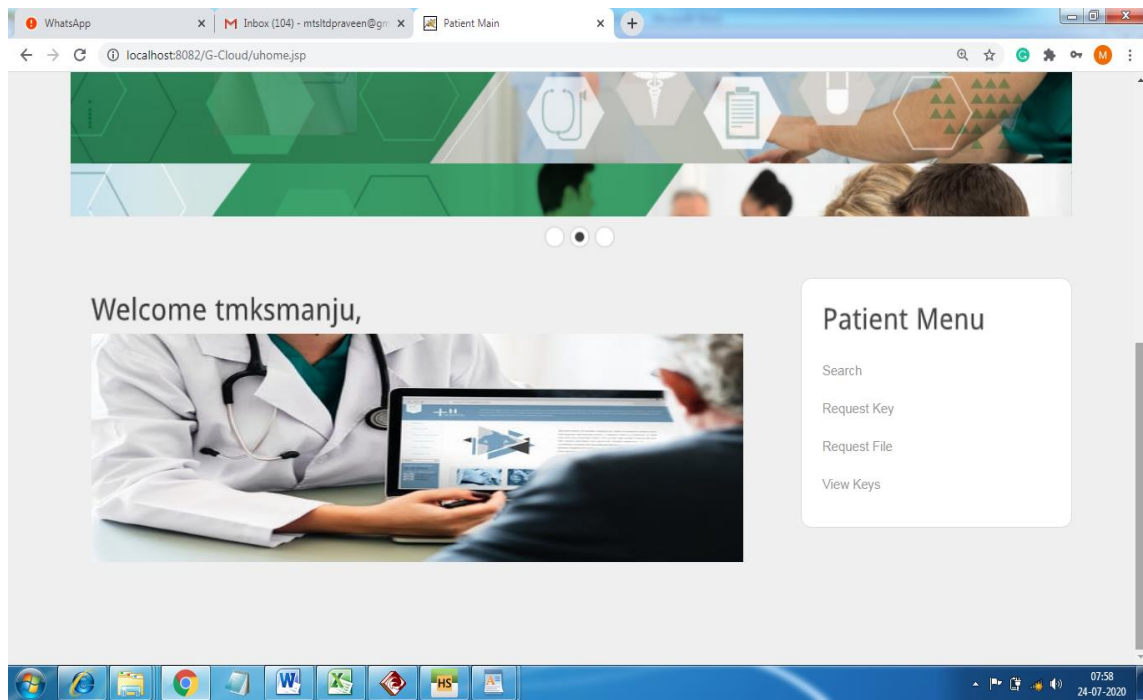
6. OUTPUT RESULTS
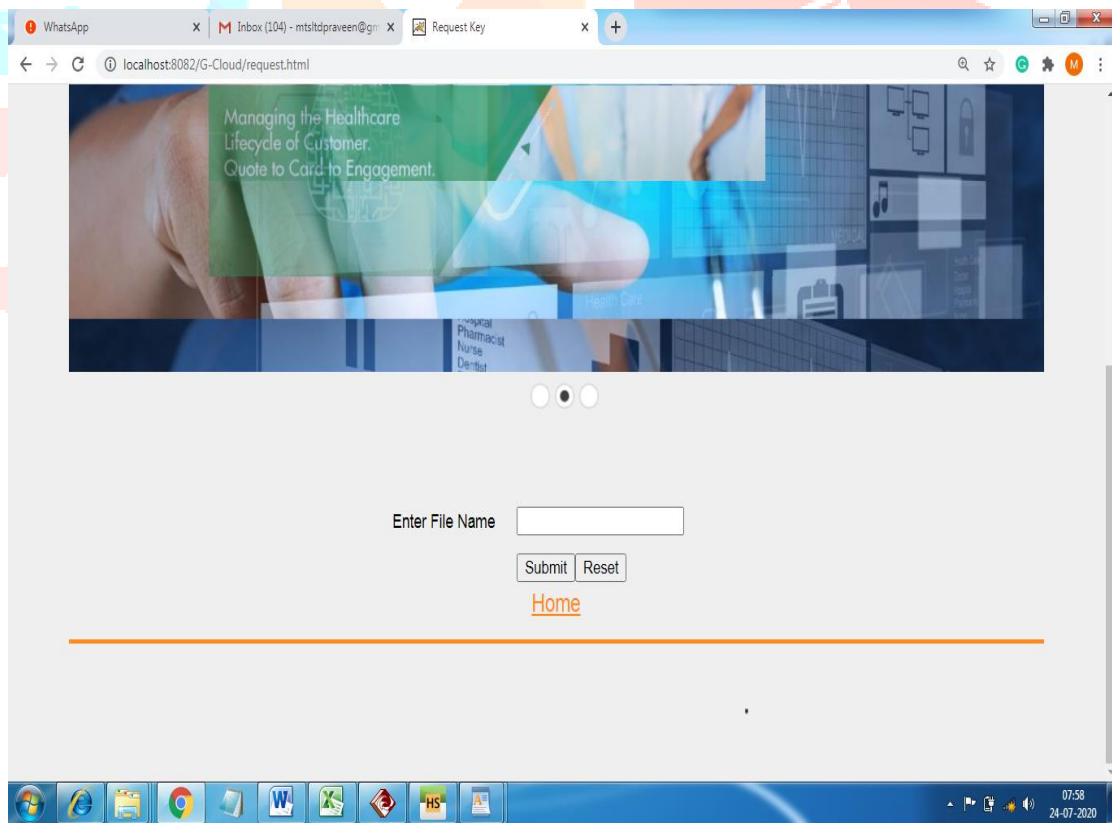
1) PKG CAN VIEW ALL PATIENTS DETAILS
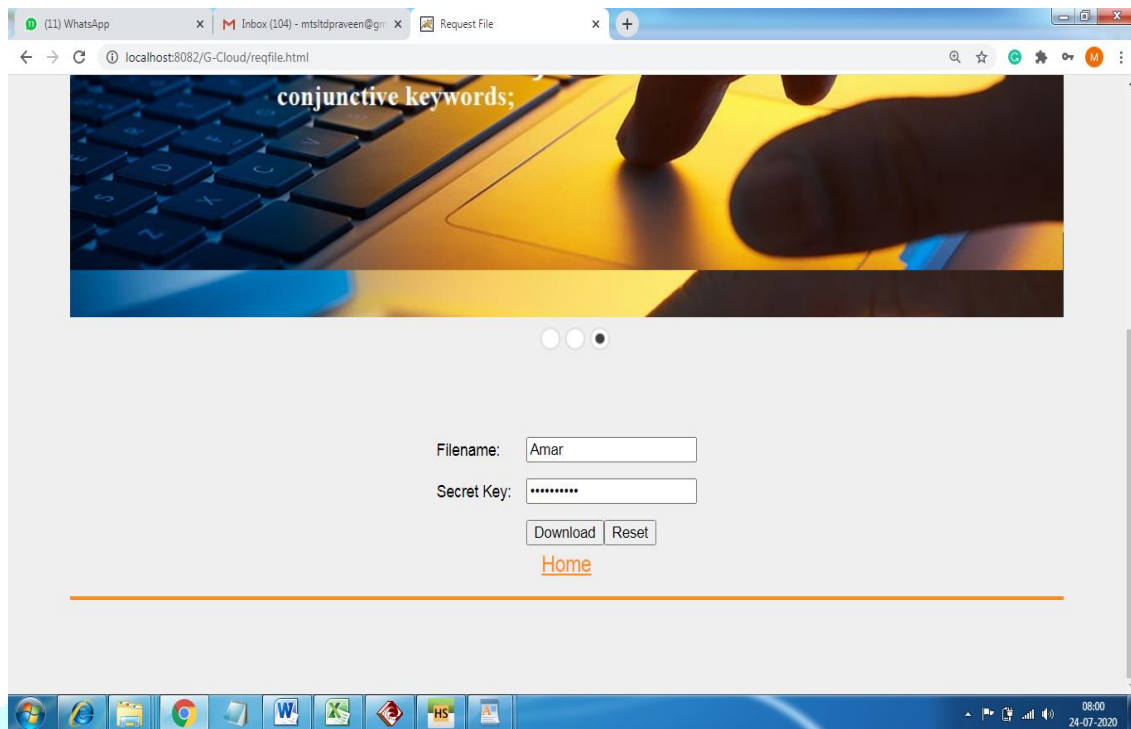

2) PKG CAN ABLE TO VIEW ALL PUBLIC KEYS

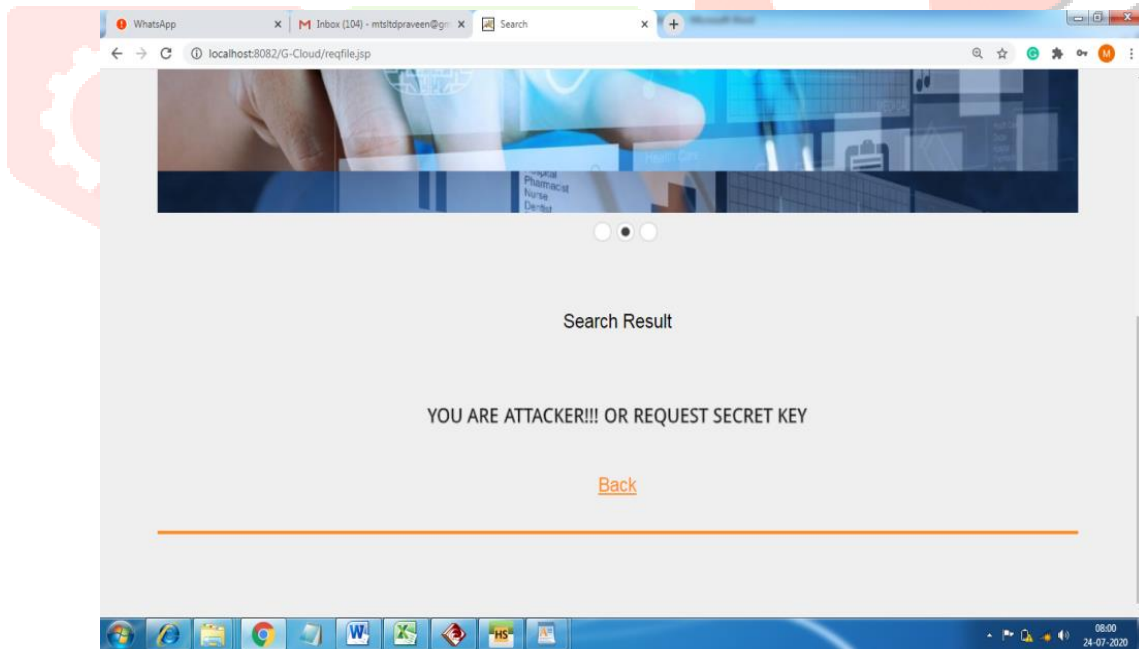## 3) PATIENTS HOME PAGE
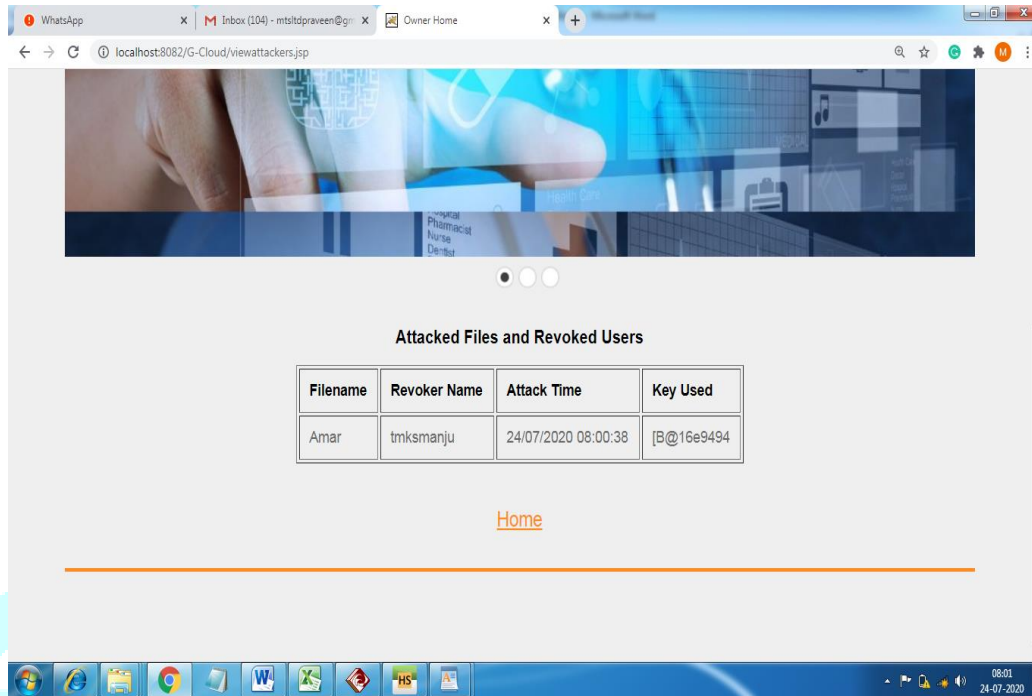

4) USER CAN REQUEST KEY

5) USER CAN DOWNLOAD THE FILE BY SUBSTITUTING VALID DETAILS

USER FAILED TO SUBSTITUTE DETAILS CORRECTLY SO HE IS IDENTIFIED AS ATTACKER

CLOUD SERVER CAN ABLE TO SEE USER DETAILS IN ATTACKER LIST

7 . CONCLUSION

In this proposed work, we proposed a secure cloud-based EHR framework that guarantees the security and privacy of medical data stored in the cloud, relying on hierarchical multi-authority CP-ABE to enforce access control policies. The proposed framework provides a high level of integration, interoperability, and sharing of EHRs among healthcare providers, patients, and practitioners. In the framework, the attribute domain authority manages a different attribute domain and operates independently. In addition, no computational overhead is completed by the government authority, and multi-factor applicant authentication have been identified and proofed. The proposed scheme can be adopted by any government that has a cloud computing infrastructure and provides treatment services to the majority of citizen patients. Future work includes implementing and evaluating the proposed scheme in a real-world environment

8. 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.

[5] Nigam, Vaibhav Kamal, and Shubham Bhatia. "Impact of Cloud Computing on Health Care." (2016).

[6] ―How to Improve Healthcare with Cloud Computing‖, By Hitachi Data Systems, white paper, (2012).

[7] Mehraeen, Esmaeil, Marjan Ghazisaeedi, Jebraeil Farzi, and Saghar Mirshekari. "Security Challenges in Healthcare Cloud Computing: A Systematic Review." Global Journal of Health Science 9, no. 3 (2016): 157.

[8] Sun, Dawei, Guiran Chang, Lina Sun, and Xingwei Wang. "Surveying and analyzing security, privacy and trust issues in cloud computing environments." Procedia Engineering 15 (2011): 2852–2856.

[9] Khan, Nabeel, and Adil Al-Yasiri. "Identifying cloud security threats to strengthen cloud computing adoption framework." Procedia Computer Science 94 (2016): 485–490.

[10] Hamlen, Kevin, Murat Kantarcioglu, Latifur Khan, and Bhavani Thuraisingham. "Security issues for cloud computing." Optimizing Information Security and Advancing Privacy Assurance: New Technologies: New Technologies 150 (2012).

[11] Omachonu, Vincent K., and Norman G. Einspruch. "Innovation in healthcare delivery systems: a conceptual framework." The Innovation Journal: The Public Sector Innovation Journal 15, no. 1 (2010): 1–20.

[12] Reddy, B. Eswara, TV Suresh Kumar, and Gandikota Ramu. "An efficient cloud framework for health care monitoring system." In Cloud and Services Computing (ISCOS), 2012 International Symposium on, pp. 113-117. IEEE, 2012.

[13] Parekh, Maulik, and B. Saleena. "Designing a cloud based framework for healthcare system and applying clustering techniques for region wise diagnosis." Procedia Computer Science 50 (2015): 537–542.

[14] Botta, Alessio, Walter De Donato, Valerio Persico, and Antonio Pescapé. "Integration of cloud computing and internet of things: a survey." Future Generation Computer Systems 56 (2016): 684–700.

[15] Stergiou, Christos, Kostas E. Psannis, Byung-Gyu Kim, and Brij Gupta. "Secure integration of IoT and cloud computing." Future Generation Computer Systems 78,(2018):964–975.

[16] Zhiwei Yu, Chaokun Wang, Clark Thomborson, Jianmin Wang, Shiguo Lian and Athanasios V. Vasilakos, A novel watermarking method for software protection in the cloud, SOFTWARE –PRACTICE AND EXPERIENCE, 42:409–430, 2012. [17] https://www.yesser.gov.sa/en/Pages/default.aspx.