www.revistageintec.net
ISSN: 2237-0722
revista GEINTEC Gestão, Inovação e Tecnologias

Secure Storage of Electronic Health Records on Cloud Using Integrity Verification Auditing

S. Srinivasan[1]; Kethineni Keerthi[2]; Gummadi Tejaswi[3]; Kodali Divya Shobana[4]

[1]Professor, Department of Computer Science and Engineering, R.M.D. Engineering College, Kavaraipettai, Chennai, Tamil Nadu, India.

[2]UG Student, Department of Computer Science and Engineering, R.M.D. Engineering College, Kavaraipettai, Chennai, Tamil Nadu, India.

[3]UG Student, Department of Computer Science and Engineering, R.M.D. Engineering College, Kavaraipettai, Chennai, Tamil Nadu, India.

[4]UG Student, Department of Computer Science and Engineering, R.M.D. Engineering College, Kavaraipettai, Chennai, Tamil Nadu, India.

Abstract

Health care facilities have tried to keep sensitive patient information safe. Health information is important in identifying any stage of treatment. However, such information should be kept confidential and only available at health care facilities. To ensure data availability, health care data is now stored in the cloud and accessible online. But, this approach poses many threats due to the possibility of a patient data to be accessed by unauthorized personnel. Moreover, the standard data access control mechanisms are insufficient to ensure integrity of data due to numerous users. The constant adjustment of privileges also affected confidentiality. This paper proposes a novel approach in which the sensitive patient data in Electronic Health Records is hidden and stored more securely in the cloud. It uses a sanitization technique to detect sensitive data in the EHR and make use of identity based shared data integrity auditing to allow authorized access to the data. The web based application which uses the proposed technique is developed and tested to demonstrate its effectiveness.

Key-words: Electronic Health Record, Cloud Computing, Cloud Storage, Sanitization, Identity Based Shared Data Integrity Auditing.

1. Introduction

Electrical Health Records (EHR) are the most important health care facilities within the world. EHRs contain important information like clinical history, allergies, blood type, genetic conditions for treating patients. Usually, a patient who needs treatment at a specialized sanatorium should ask his or

her own doctor to send his or her medical records to a replacement physician. However, this procedure is time consuming, complicated and, in some cases, impossible if the patient is unconscious. it's extremely difficult to use policies that allow health care facilities to share patient information because of complex systems, asset plans, legislation and software restrictions. Lohr, et al. propose an answer backed by reputable and reliable sources. Health care facilities can use a unified domain to share access to their services. This solution provides access to patient data but limits access to the chosen patient. Once the middle was given access to the system, we could read all of its records. This freedom of entry violates several privacy concerns. Patient data (EHR) should be shared but mustn't be available at any facility; it's unfeasible to use one web system for all health care facilities and its patients. Using Cloud Service Providers (CSPs) to store and manage EHR access is taken into account the most effective solution. In this way, each health care facility can still use its own operating systems but rather than storing the patient's location data, we are able to store and access it using the general public cloud. Public cloud services are ready to measure and supply availability because they'll be available through the online. Using public clouds rather than using in-house data centers also can reduce costs. Typically, Electronic Health Records (EHRs) are stored and shared within the cloud containing sensitive patient information (patient name, signal and ID number, etc.) and hospital critical information (hospital name, etc.). When EHRs are uploaded to the cloud directly for research purposes, sensitive patient and hospital information could also be disclosed to unauthorized users. Otherwise, the integrity of EHRs must be verified because of human error and software / hardware failures within the cloud. Therefore, it's important to hold out remote data reliability tests on the condition that sensitive shared data be protected.

This paper proposes a brand new way of empowering the storage of EHRs publicly clouds. It focuses on ensuring the confidentiality and integrity of EHRs. This model provides security for several countries without increasing the issue of controlling the roles and groups of users. It uses a cleanup process to spot the foremost sensitive information in a very record and to guard it using signatures. It are often easily used and installed on any cloud-based web applications. The rest of this paper is organized as follows. Section 2 describes the activities associated with EHR protection. Section 3 describes the structure of the system and describes each component and the way they work together. Section 4 presents the launch details and Section 5 concludes this paper.

2. Related Works

To ensure the authenticity of the info stored within the cloud, variety of information testing programs are proposed. to scale back the pc burden on the user side, a third-party Auditor was introduced to verify the authenticity of cloud information on behalf of the user. Ateniese et al. first I suggested the Provable Data Possession to confirm that information is accessible in an unreliable cloud [10]. In their proposed scheme, homomorphic authorities and sampling techniques tend to get unhindered verification and reduce I / O costs. Juels and Kaliski described a model called Proof of Retrievability and proposed an efficient system [3]. during this scheme, the info stored within the cloud is commonly restored that the integrity of that data is commonly verified. supported by BLS pseudorandom and BLS signature, Shacham and Water have proposed a system for investigating data integrity removed from a public remote data research scheme [4]. To protect privacy information, Wang et al. proposed a confidential privacy research program employing a random encryption method employing a special additional encryption process to further develop an external data integrity audit system that supports data privacy protection [5]. To reduce the overhead of computer signature processing on the user side, Guan et al. develops a system for researching the integrity of foreign data to support a non-discriminatory process. Shen et al. introduced the 3rd Party Medium (TPM) to include a simplified scheme of research for light weight information [8]. in line with the program, TPM assists the user to get signatures on the condition that the information privacy is protected so as to support data capabilities. Many of the available methods have two important limitations as given below:

i. The employment of Public Key Infrastructure (PKI) goes beyond the emergence of complex certification management.

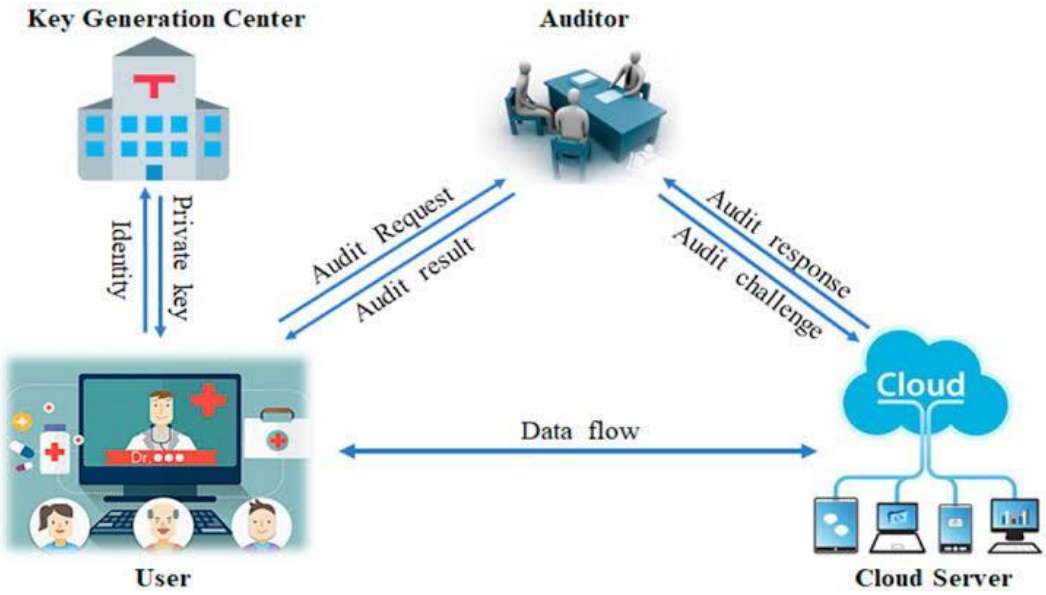
ii. Existing data integrity schemes don't support data sharing by encrypting sensitive information.

3. Proposed System

The design of the proposed system is illustrated in Fig.3.1 The proposed system explores the way to achieve data sharing with sensitive data hidden in remote data research, then proposes a substitute for identity-based data auditing with sensitive information hidden in secure cloud storage. Shared data analytics scheme is suggested for secure cloud storage. The sanitizer is employed to scrub info blocks as sensitive file information. First the user blinds the knowledge blocks because the confidential information of the first file and generates the corresponding signatures, then sends it to

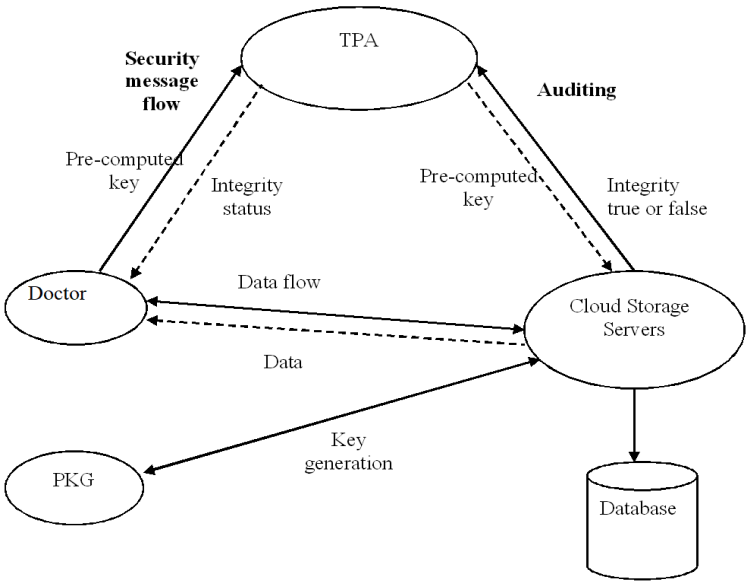
the sanitizer cleaner. The sanitizer cleaner cleans these blind data blocks in an exceedingly consistent format and also cleans the knowledge blocks as sensitive organizational information. It also converts the identical signatures into an invalid file. This method not only detects remote data testing, but also supports the sharing of knowledge within the event that sensitive data is shielded from cloud storage.

Figure 3.1 - System Architecture



The data flow in the proposed system is depicted in the Fig.3.2.

Figure 3.2 - Work Flow of the System



Received: 08.04.2021 – Accepted: 30.04.2021

The proposed system has many advantages.

1. Sensitive information can only be protected when non-sensitive information is published.

2. It enables the file stored inside the cloud to be shared and utilized by many others easily.

3. because it uses remote data integrity analysis, the information within the EHR remains consistent.

4. When encryption was wont to protect patient data and hospital data, EHRs couldn't be easily utilized by most investigators. This problem is being addressed within the proposed way.

4. Implementation

The entire concept is implemented and incorporated in a web based application. The application was implemented using Java Server Pages (JSP) and developed on a platform with Intel Core Duo, Windows 10 Operating system with 2GB RAM. The following figures from 4.1 to 4.11 showed the screen shots of key aspects in the proposed approach.

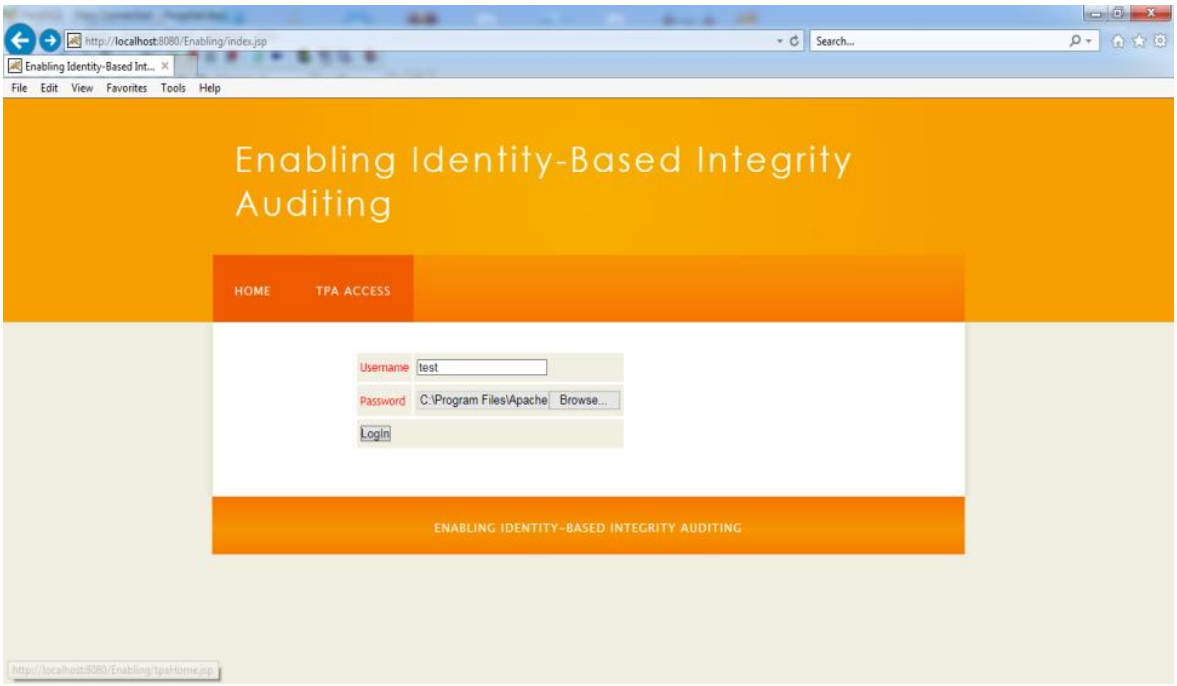
i. EHR Creation

ii. Blinded File Creation

iii. Sanitization

iv. Publication of EHR Files

Figure 4.1 - Authentication Module



Received: 08.04.2021 – Accepted: 30.04.2021

Figure 4.2 EHR Creation

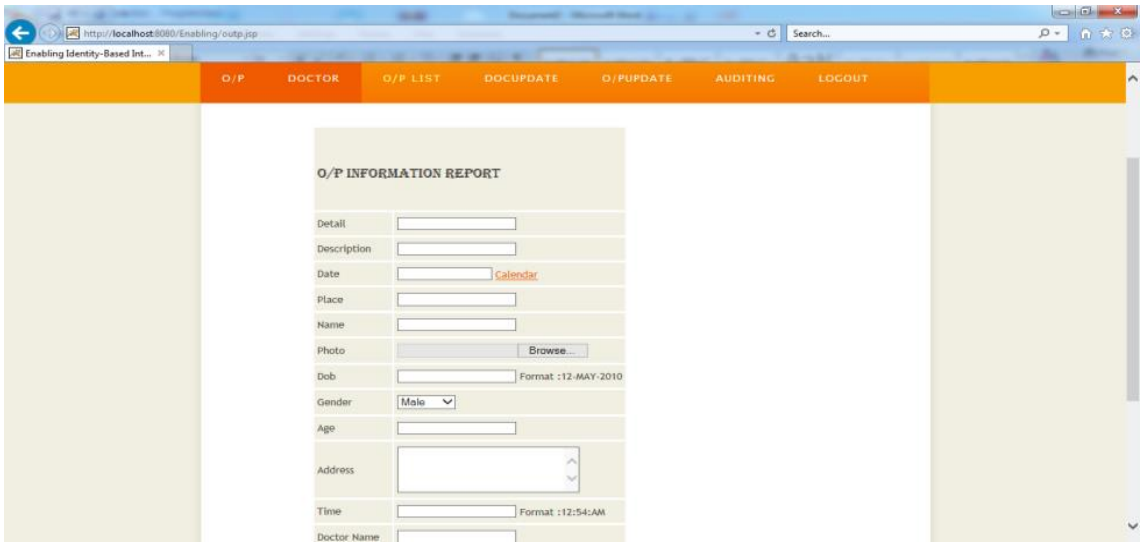


Figure 4.3 - EHR Creation

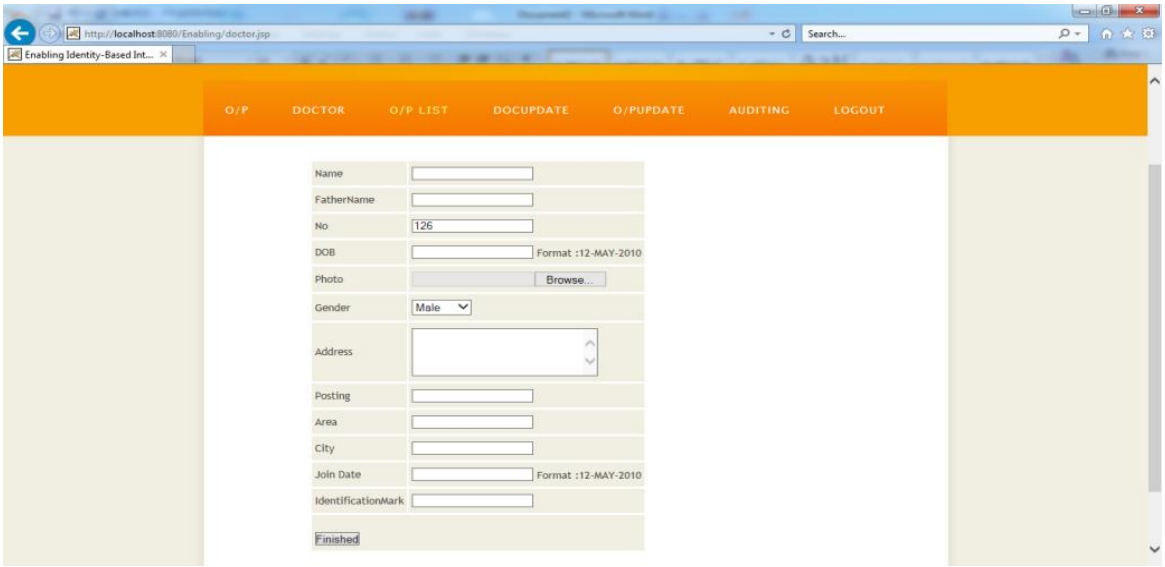
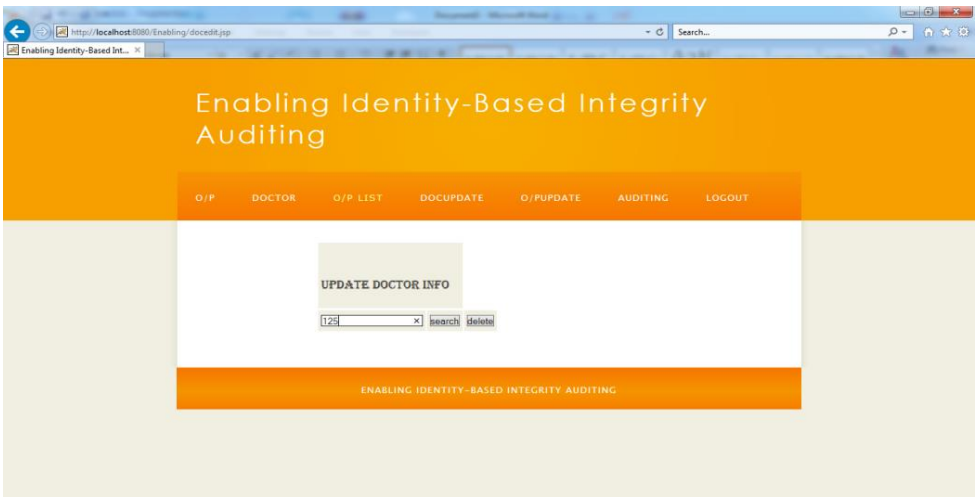


Figure 4.4 - Doctor Information in EHR



Received: 08.04.2021 – Accepted: 30.04.2021

Figure 4.5 - Doctor's Data in EHR

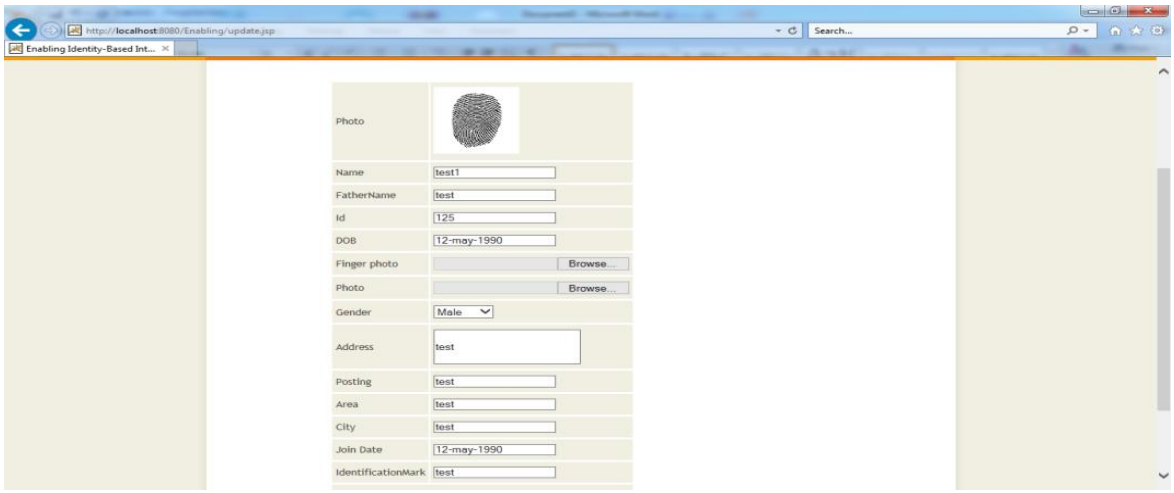


Figure 4.6 - Implementation of Sanitization

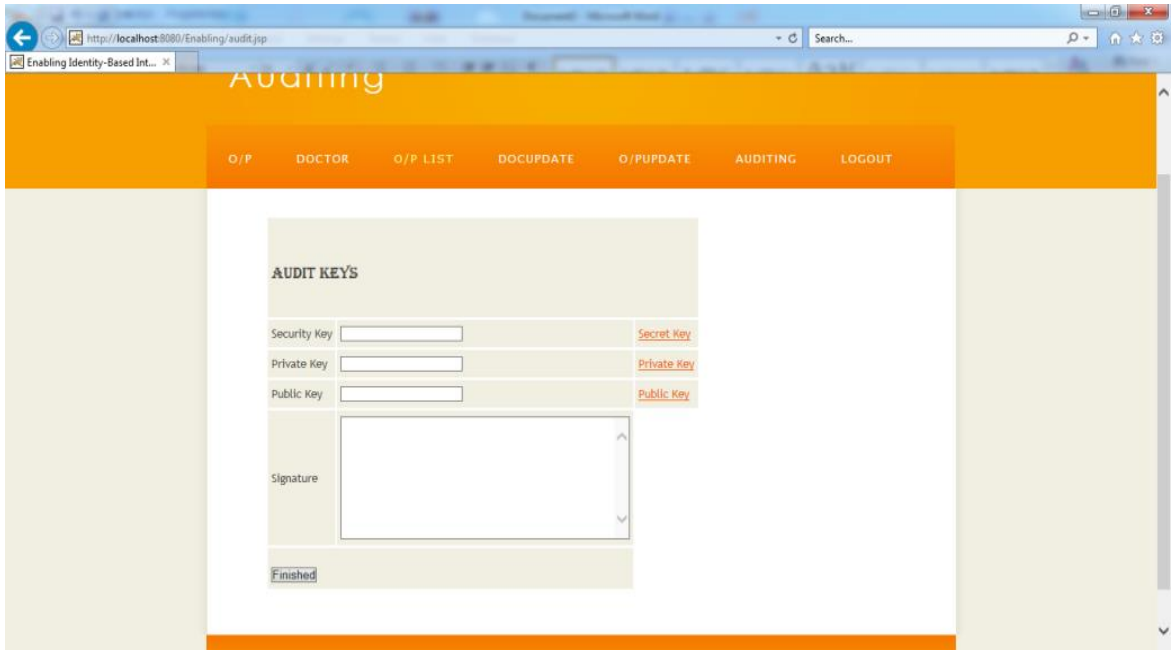
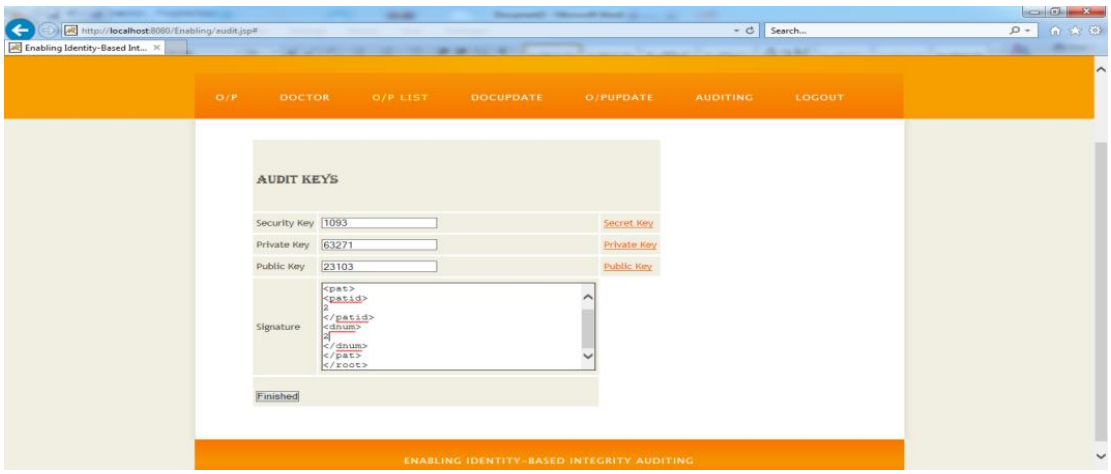


Figure 4.7 - Implementation of Identity based Integrity Auditing



Received: 08.04.2021 – Accepted: 30.04.2021

Figure 4.8 - Auditing EHR

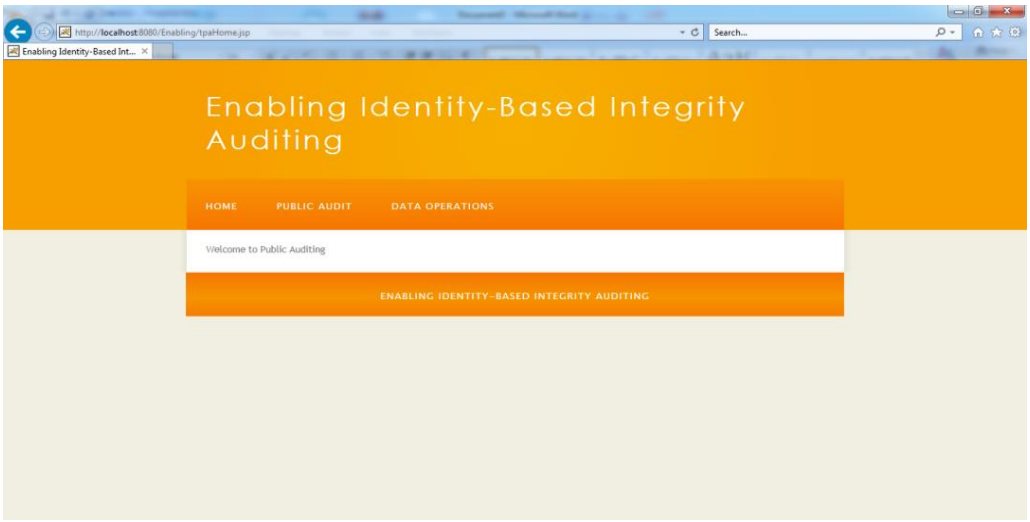


Figure 4.9 - Validating EHR

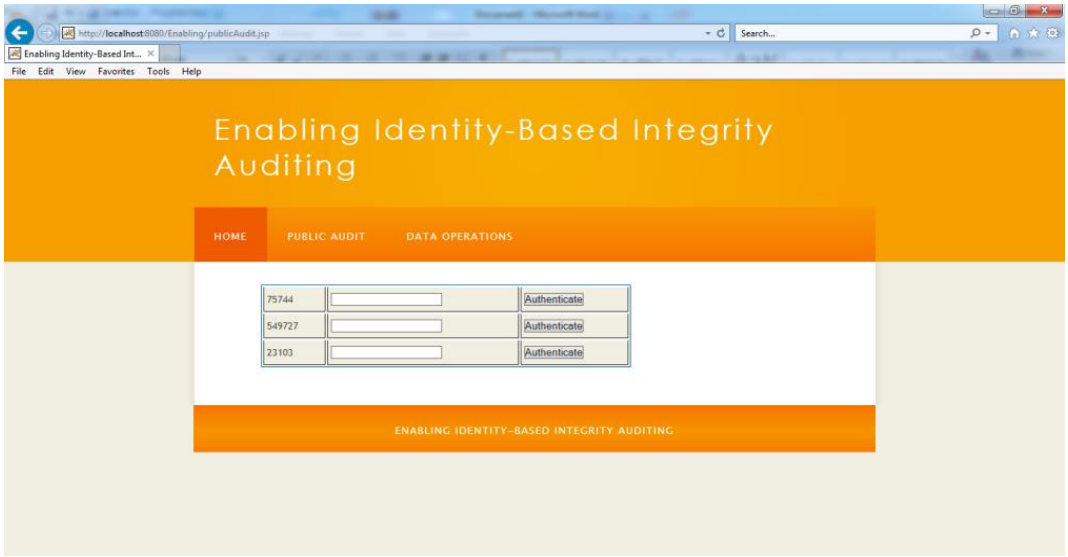


Figure 4.10 - Ensuring Data Integrity

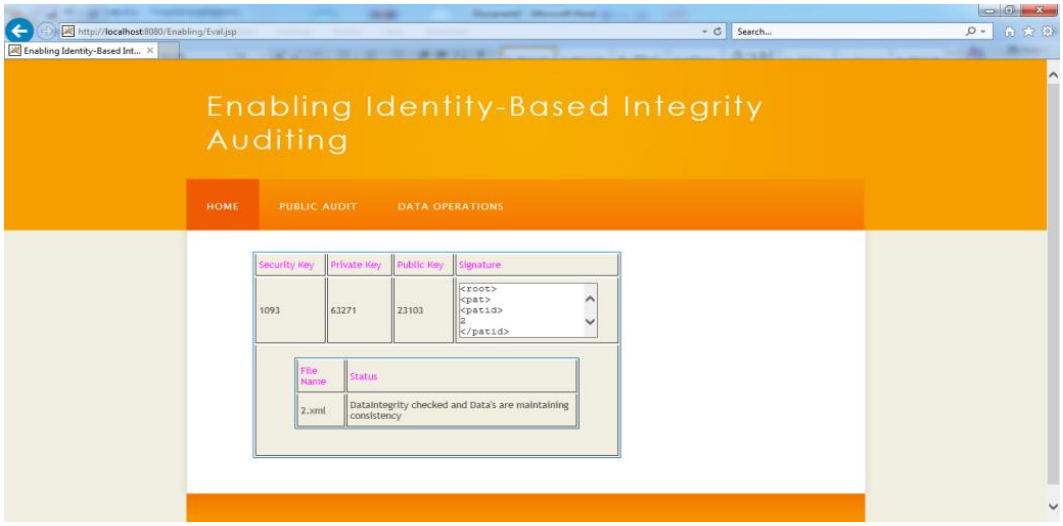
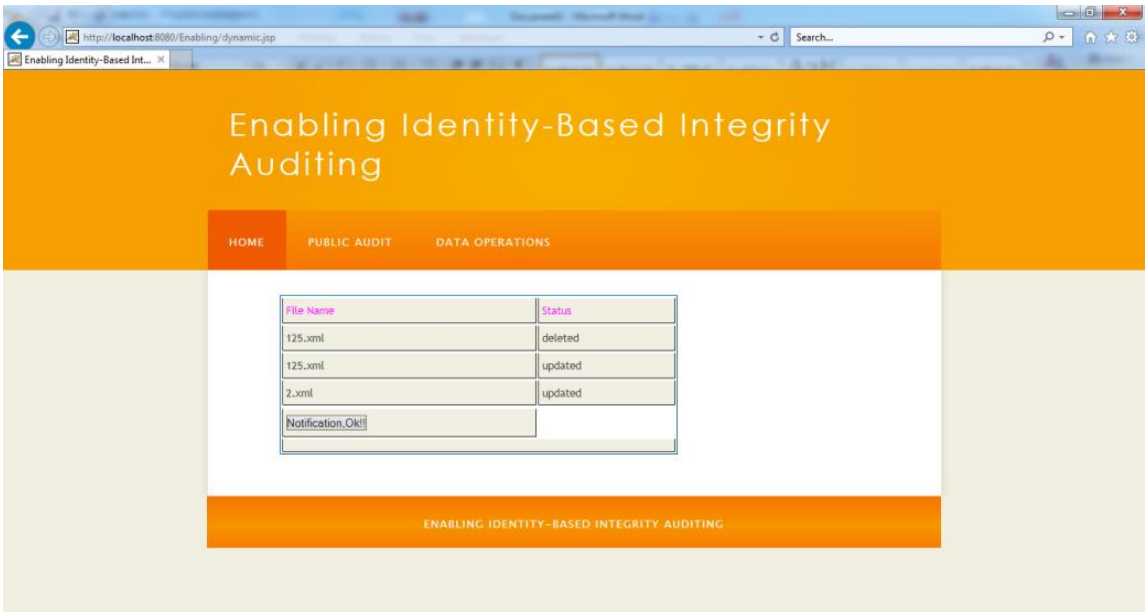


Figure 4.11 - EHR Files in Cloud Storage



5. Conclusion

This paper proposes an ID-based data integrity monitoring system for secure storage and sharing of sensitive information in the EHR. In this way, EHRs stored in the cloud can be shared with anyone who guarantees that sensitive file details will not be altered. Besides, remote data reliability research can still be done efficiently. Proof of safety and thus the test analysis shows that the proposed system achieves the desired safety and performance. In the future, the app will use the Merkle Hash Tree (MHT) authentication structure to properly and securely ensure that a group of elements is not damaged and altered.

References

Ren, K., Wang, C., & Wang, Q. (2012). Security challenges for the public cloud. *IEEE Internet computing*, *16*(1), 69-73.

Ateniese, G., Burns, R., Curtmola, R., Herring, J., Kissner, L., Peterson, Z., & Song, D. (2007). Provable data possession at untrusted stores. In *Proceedings of the 14th ACM conference on Computer and communications security*, 598-609.

Juels, A., & Kaliski Jr, B.S. (2007). PORs: Proofs of retrievability for large files. In *Proceedings of the 14th ACM conference on Computer and communications security*, 584-597.

Shacham, H., & Waters, B. (2013). Compact proofs of retrievability. *Journal of Cryptology*, *26*(3), 442–483.

Wang, C., Chow, S.S., Wang, Q., Ren, K., & Lou, W. (2011). Privacy-preserving public auditing for secure cloud storage. *IEEE transactions on computers*, *62*(2), 362-375.

Received: 08.04.2021 – Accepted: 30.04.2021

Worku, S.G., Xu, C., Zhao, J., & He, X. (2014). Secure and efficient privacy-preserving public auditing scheme for cloud storage. *Computers & Electrical Engineering*, *40*(5), 1703-1713.

Guan, C., Ren, K., Zhang, F., Kerschbaum, F., & Yu, J. (2015). Symmetric-key based proofs of retrievability supporting public verification. *In European symposium on research in computer security*, 203-223.

Shen, W., Yu, J., Xia, H., Zhang, H., Lu, X., & Hao, R. (2017). Light-weight and privacy-preserving secure cloud auditing scheme for group users via the third party medium. *Journal of Network and Computer Applications*, *82*, 56-64.

Sun, J., & Fang, Y. (2009). Cross-domain data sharing in distributed electronic health record systems. *IEEE Transactions on Parallel and Distributed Systems*, *21*(6), 754-764.

Ateniese, G., Di Pietro, R., Mancini, L.V., & Tsudik, G. (2008). Scalable and efficient provable data possession. *In Proceedings of the 4th international conference on Security and privacy in communication netowrks*, 1-10.

Löhr, H., Sadeghi, A.R., & Winandy, M. (2010). Securing the e-health cloud. *In Proceedings of the 1st acm international health informatics symposium*, 220-229. https://doi.org/10.1145/1882992.1883024