Secure Cloud Storage and Sharable for Electronic Health Records Using Encryption Techniques

[1] Pindi Venkanna, [2] CH. Suresh

[1] MCA Student, Dept. Of MCA, Swarnandhra College of Engineering and Technology, Seetharampuram, Narsapur, Andhra Pradesh 534280,

pindivenkannababu17@gmail.com

[2], Assistant Professor, Dept. Of MCA, Swarnandhra College of Engineering and Technology, Seetharampuram, Narsapur, Andhra Pradesh 534280,

***Abstract**: Due to the capability of information breaches and the consequent compromise of affected person's touchy facts, clinical corporations discover it difficult to comfy the statistics stored on cloud garage. Thus, storing and sharing information on cloud presents several security issues related to authentication, identity control, get admission to manage, believe control and so forth. Electronic Health Records (EHR) is of the paramount importance inside the area of studies as the researchers use these facts/reports to investigate and discover new illnesses. EHR data saved on cloud incorporate sensitive facts approximately the patient and cannot be disclosed to unauthorized users. Thus, sharing touchy statistics continues to be remains unexplored. Therefore, this newsletter proposes a unique framework to store and share the information in a secured manner the use of Attribute Based Encryption (ABE). S touring and sharing EHR data at the cloud lets in the studies community to analyze numerous affected person reports, which intern helps pharmacy and other healthcare -agencies to increase their business.*

Keywords— *Cloud Storage, EHR, Firebase, Cloud storage*

I. INTRODUCTION

EHR is popularly known as medical IT machine and are used to save a affected person's clinical statistics, inclusive of their clinical history, modern medications, test outcomes, descriptions of any precise or ongoing conditions, vaccination information, ultrasound scan findings, x-ray pictures and so forth. EHR marketplace cap is e expected to increase from $24.Eighty two billion in 2018 to $37.Thirteen billion by way of 2025 [1]. Patient facts are controlled via an expansion of digital health document systems, for example cloud-based, server-primarily based software's. A cloud- based

EHR makes use of cloud garage era to shop, proportion, and shield affected person sensitive facts. Cloud storage additionally gives fast, flexible, scalable, and cost-effective in restructure for storing records. The Health Insurance Portability and Accountability Act (HIPAA) have defined the following safety necessities that should be accompanied by way of hospitals whilst dealing with health records generation [2].

1. Authorized get entry to: Services for relaxed records storage and authorized get right of entry to be furnished by cloud storage.

HIPAA regulations advocate healthcare companies to properly display screen personnel who will have access to patient information and to hold music of their get admission to codes.

2. Patient's consent: A patient need to be privy to how their scientific statistics is treated safeguarded, and who has get admission to it.

3. Archiving: Patients clinical statistics is saved for a certain duration time and then it should be deleted by using legal personnel.

HIPAA mainly focuses on the necessities to make certain the confidentiality, integrity, and availability of the data stored on cloud. However, this paper concentrates best on confidentiality.

The cloud presents large storage and computation sources to manage the EHR statistics. However, after outsourcing their statistics to the cloud, the statistics owners now not have physical control over it. Data safety and privacy is now a chief fear for facts owners when you consider that they now not have physical manipulate over their information after outsourcing it to the cloud and, greater crucially, due to facts leakage. Traditional encryption techniques may be used to shield data confidentiality; however they're no longer very effective for accommodating bendy facts sharing necessities. Thus, ABE is used to obtain and keep records confidentiality.

Thus, our proposed work allows cloud customers including researchers can use cloud EHR statistics in a secured manner. Health research is an critical difficulty in each healthcare and drug discovery businesses to improve human fitness. Health studies can also benefit in new remedies, higher diagnostics, and prevent infection.

The relaxation of this paper is prepared as follows: Section II describes associated work. In Section III proposed model is discussed. Section IV describes implementation of proposed framework. Section V overall performance evaluation of proposed algorithm is discussed; effects are mentioned in phase VI. Section VII concludes the proposed studies work.

II Related work

Authors in [3] have given an insight approximately how cloud garage become significantly used by numerous businesses and also how data may be shared with various customers. Proposed framework consists of the advent of a collection manager as authenticator. This authenticator method ensures the privateers of data with the aid of the usage of blind signature method. Data safety using RSA partial homomorphism m (RSAPH) and MD5 Cryptography (md 5C) is proposed in [4]. Here whole facts are encrypted using RHAPH before its far being uploaded on to the cloud. Here MD5 is used to generate Hash value. Finally, consumer can decrypt facts the usage of a personal key which turned into generated first of all. In [5], authors have offered a critical security difficulty related to the e exposure of key. Here a customer constantly updates their secret key that's in the end will increase the weight on them. In order to reduce the load on the purchaser and to make key replace procedure transparent. Authors in [6] gift solutions related to cloud computing technologies. Detailed protection evaluation is carried out on shared cloud statistics and solutions for the equal are discussed. Different models supplied in [7] to conquer the statistics integrity trouble in conjunction with their execs and cons. Wang et al. [8] proposed a framework known as Panda, a signature is attached to every facts block and whilst a user modifies the block a brand new signature is computed and attached. This prevents the revoked user from having access to the statistics. Provable Data Possession (PDP) is provided in [9] to make sure the information ownership on entrusted cloud. Shen et al.

[10] Presented a Third-Party Medium (TPM), TPM assists a consumer with growing marks relying on the consumer prerequisite. Signatures are generated proper earlier than importing the records directly to the cloud or another platform. Similarly, a unique public scheme is proposed in [11] to incorporating group signature for records blocks. Furthermore, random protecting techniques are used to guard statistics from TPA. Square chain innovation with the important thing less signature is utilized in [12]. Prior to moving information directly to the cloud, the safety problems should be alleviated [13]. A non- cryptographic manner to deal with ECG data privacy is proposed in [14]. The proposed architecture has labelled the patient's cardiovascular facts and anonym zed facts utilising the PRD. Authors in [15]

reviewed the techniques which are presently used to protect the safety and privateers of cloud-primarily based EHRs and additionally analyzed the security and privacy problems together with boundaries. A approach for transferring the executive burden of dealing with offerings from the affected person to the healthcare corporation is presented in [16] and facilitating easy delegation of the cloud-based totally EHR's get admission to rights to the healthcare specialists

. Patient records safety is proposed in [17]. Matos et al.

[18] Affords architecture the use of haze of mists method. Research article [19] proposes a framework by way of using STRIDE modelling tool to version threats posed via EHR machine and the amount of threat is calculated the use of DREAD. In order to address safety and privacy issues in e- Health, Sivan, R. Et al. [20] reviewed recent and prior literature on numerous strategies and mechanisms.

III Proposed Model

Proposed architecture is as shown in Fig.1. System model contains following modules patients, doctor/admin, sanitization, user authentication and key management, researchers etc.

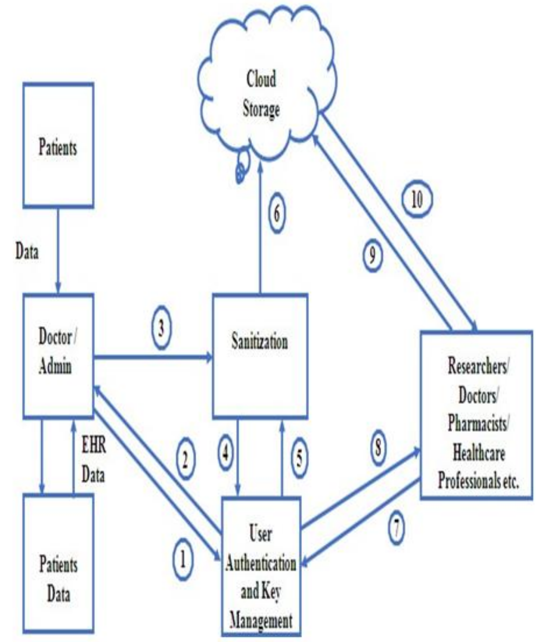

Cloud Storage
Patients
Data
Doctor/ Admin
3
Sanitization
6
10
9
Researchers/ Doctors/ Pharmacists/ Healthcare Professionals etc.
EHR Data
2
4
5
8
7
1
Patients Data
User Authentication and Key Management

Fig.1: system model

1. Illustrates various steps concerned within the procedure collecting, hiding private facts, storing secured information on cloud and allow the records visitors/analyzers to download the EHR facts.

Registered customers (Doctors/ admin) might be authenticated in steps 1 and a pair of. In step 3 patients' touchy data is sanitized. During the manner of sanitization replace the statistics is changed with a digital signature generated by means of key management module (steps 4 and five) and in step 6 sanitized information is stored on cloud. Registered data viewer/analyzers may be authenticated and for a requested report OTP may be sent in steps 7 and eight. Finally information analyst can download the statistics in steps 9 and 10. Thus, the affected person's private records (sensitive) can be secured and the other statistics can be shared on cloud.

Fig.2 suggests the person authentication model used in the consumer authentication and key management module. All registered customers are proven via authentication modules of Firebase Open ID Connect (OIDC) authentication and authorization machine.

Doctor/administrator collects patients and generates EHR Here patient's data is saved on the Firebase Real time database which synchronizes information across all the legal users. Five entities used in our proposed system are Cloud Storage, Patient, Data sanitization, Authentication and key control information recipients.

� Patient: The patient is the facts proprietor in their EHR and establishes the get right of entry to hints for statistics customers.

� Cloud garage: health practitioner/admin can upload the Patient's facts and proportion their records with others.

� Sanitization: Patient sensitive facts are changed with a corresponding digital signature stored on cloud. Our proposed technique makes use of ECDSA (Elliptic Curve Digital Signature Algorithm) algorithm to generate a digital signature based on the elliptic-curve cryptography (ECC).

� User authentication and key management: Firebase Authentication modules are used for consumer authentication reason

• Data recipients: all information receivers are registered customers. Only registered users can study and examine the facts based OTP they get hold of.

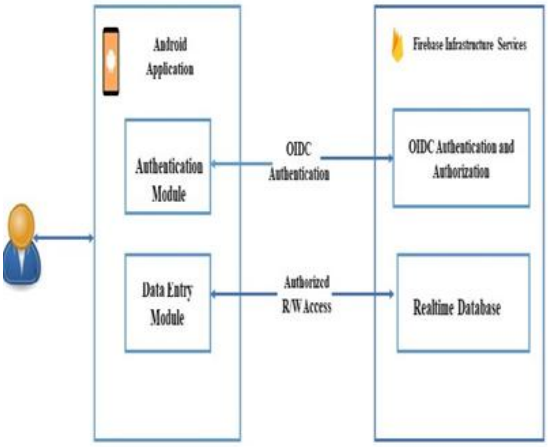


Fig.2: User Authentication

Fig.3 is the Use-Case diagram which displays the interactions among users and the application of the system. The doctor who is an authorized user uploads the medical report after blinding and sanitizing the personal sensitive information to the cloud, which can be retrieved by the patient. The admin manages the user logs and provides authorization to the genuine researchers. Researchers can download the report after receiving one-time password (OTP).

IV Implementation

The implementation of proposed framework contains frontend and backend modules. The front end is a user interface, while back end is the server, application, database and cloud storage.

Front End

Android studio and XML is used to implement front end modules. The front-end module consists of an admin and three end users. The end users are doctor, patient and the researcher. Admin is just like the administrator of the hospital; it can add users, authenticate users and also permit the genuine researcher. All these operations are recorded stored on cloud storage.

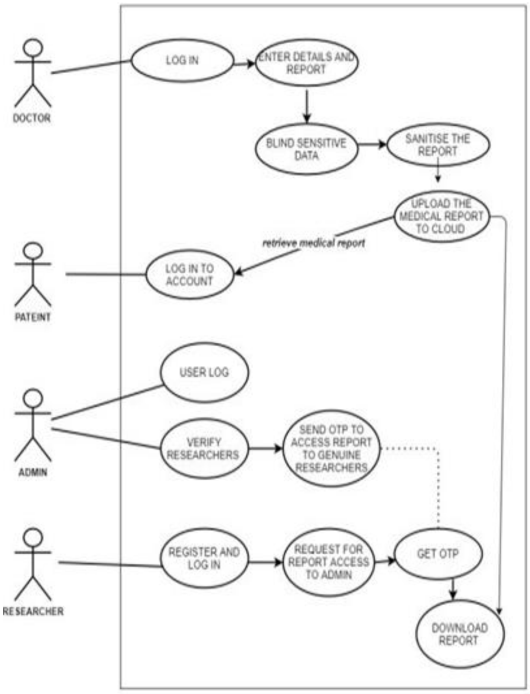


Fig.3: Use-Case Diagram

Doctor

The medical doctor uploads the patient's electronic health reports. While uploading patient's record, data is blinded patient's sensitive information and it also generates the corresponding signatures. Once patient sensitive information is blinded, it is sent for the information hiding module. Finally, encrypted data is then uploaded or stored in the Cloud storage.

Researcher

Cloud admin authenticates and permits researchers to view/download the reports. For downloading the report, a secret key is sent to the researcher through the One Time Password (OTP).

Patients

Patient can also view/download the uploaded data.

Back End

At Back End, Firebase SDK database and Cloud Fire store is used. There is much demand for Firebase in creating mobile and web applications. By using Firebase, we can host servers, can check for user' authenticity, and can achieve password security among many others. The Firebase real- time database is a NoSQL database. In Firebase, the data is stored as JSON and synchronized in real-time to every connected client. Due to the flexibility, scalability and real-time characteristics of the firebase, it is considered as a best choice to create database for the proposed application.

User Authentication and authorization

Our application will never let any random users to login and access data stored on cloud storage. All types of users are authenticated to identify users is genuine or not. Well, Firebase helps us do the e xact same thing. The application collects the user's identity and stores it securely in the cloud storage which can be accessed only by the administrator. This authentication can be achieved easily using SDKs and well-equipped UI (User interface) libraries.

Algorithm

Digital signature is generated by ECDSA algorithm. ECDSA is a secured digital signature algorithm based on ECC. Generating digital signatures involves two Phases.

Phase1: Key Generation

The ECDSA algorithm contains a private key and a public key. Public key is a point on an elliptic curve, while private key is an integer. The private key is a random integer number in the range [0,...,n-1], Where n is subgroup of EC (Elliptic Curve) points. The public key is generated by a multiplication point on Elliptic Curve *pubKey = privKey * G.*

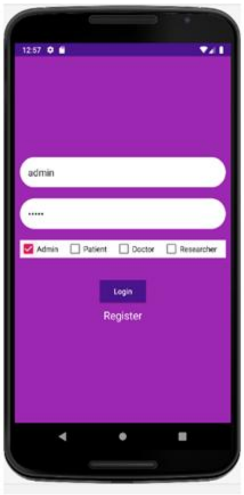
Phase2: Digital signature generation

The ECDSA algorithm is based on the ElGa mal signature scheme. This algorithm returns a signature.

1. Find hash for a given message, using a hash function (h).
2. Find a random number k in the range $[1, .. n\text{-}1]$.
3. Determine a random point on elliptic curve
   $(x_1, y_1) = K * G.$
4. *Find* r = R X x_1 If $r=0$, go to step 2.
5. Calculate $s = k^{-1} *(h + r * privKey)\ mod(n)$
6. return Signature (r,s)

V RESULTS

Proposed framework is implemented as android mobile application. The mobile application uses Android SDK to implement proposed methodology. Various screenshots of our mobile application implementation is as show in Fig.4to Fig .14.


12:57

admin

•••••

☑ Admin □ Patient □ Doctor □ Researcher

Fig.4: user login

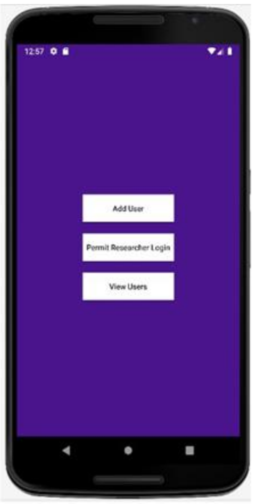

12:57

Fig.5: Admin login

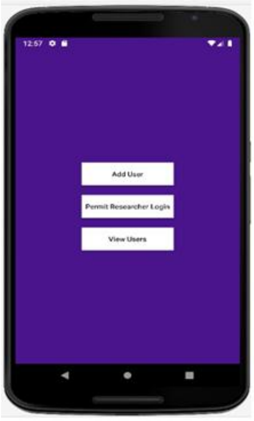
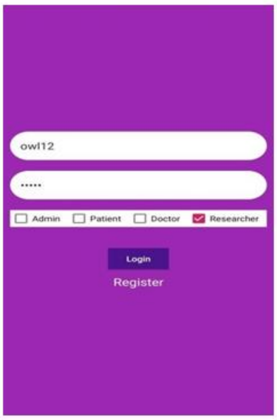

12:57

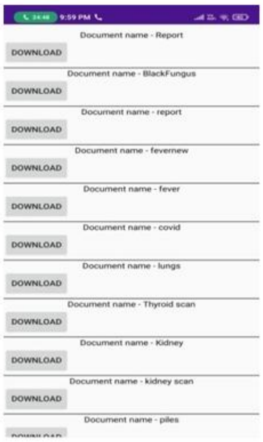
Fig.10: Authorize researcher


owl12

•••••

□ Admin □ Patient □ Doctor ☑ Researcher

Fig, 11: Researcher Login


9:59 PM

Document name - Report

DOWNLOAD

Document name - BlackFungus

DOWNLOAD

Document name - report

DOWNLOAD

Document name - fevernew

DOWNLOAD

Document name - fever

DOWNLOAD

Document name - covid

DOWNLOAD

Document name - lungs

DOWNLOAD

Document name - Thyroid scan

DOWNLOAD

Document name - Kidney

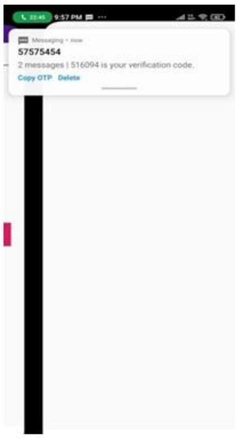
DOWNLOAD

Document name - kidney scan

DOWNLOAD

Document name - piles

Fig.12: Download report

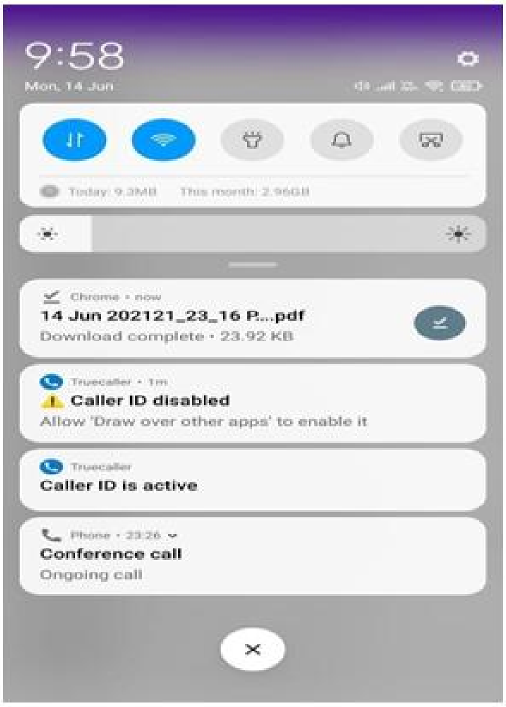

9:57 PM

Messaging • now

57575454

2 messages | 516094 is your verification code.

Fig.13: Receiving the OTP


9:58

Mon, 14 Jun

Today: 9.3MB This month: 2.96GB

Chrome • now

14 Jun 202121_23_16 P...pdf

Download complete • 23.92 KB

Truecaller • 1m

Caller ID disabled

Allow 'Draw over other apps' to enable it

Truecaller

Caller ID is active

Phone • 23:26

Conference call

Ongoing call

Fig.14: Report downloaded

VI CONCLUSION

This article has proposed a framework for sharing patient's touchy facts amongst one of kind sorts of users. Proposed framework encrypts patient's sensitive records in opposition to publishing and uploads information to be shared on to the cloud. Finally encrypted patients' information is saved on cloud garage. If the sensitive records within the EHR are protected, then the EHR saved inside the cloud can be shared and used with the aid of others (researchers, statistics analysts, and so forth.). Users should reap a prior permission from admin to download and use the statistics. This work can be e extended through adding extra functions like categorization of the fitness reports based at the sort of illnesses so as to be lots less complicated and faster for the researcher to get reviews based on a unique ailment.

REFERENCES

[1]. https://cprimestudios.com/blog/benefits-and-challenges- cloud-based-electronic-health-record.

[2]. U.S. Department of Health and Human Services, Summary of the HIPAASecurity Rule https://www.hhs.gov/hipaa/for-rofessionals/ security/laws- regulations/ index.html.

[3]. G. Yang, J. Yu, W. Shen, Q. Su, Z. Fu, and R. Hao , Enabling public auditing for shared data in cloud storage supporting identity privacy and traceability, Journal of Systems and Software, 2016.

[4]. P. Ora and P. R. Pal, Data security and integrity in cloud computing based on RSA partial homomorphism and MD5 cryptography, International Conference on Computer, Communication and Control, 2016.

[5]. J. Yu, K. Ren, and C. Wang, Enabling cloud storage auditing with verifiable outsourcing of key updates, IEEE Transactions on Information Forensics and Security, 2016.

[6]. Aldossary, Sultan & Allen, William, Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions, International Journal of Advanced Computer Science and Applications, 2016.

[7]. Thakur, Neha & Sharma, Aman, Data Integrity Techniques in Cloud Computing: An Analysis, International Journal of Advanced Research in Computer Science and Software Engineering, 2017.

[8]. Wang B, Li B, Li H Oruta: privacy-preserving public auditing for shared data in the cloud. IEEE Trans Cloud Comput 2(1), pp 43–56, 2014.

[9]. G. Ateniese et al., Provable data possession at entrusted stores," in Proc. 14th ACM Conf. Computer Communication Security., pp. 598–609, 2007.

[10]. W. Shen, J. Yu, H. Xia, H. Zhang, X. Lu, and R. Hao, Light-weight and privacy-preserving secure cloud auditing scheme for group users via the third-party medium, J. Netw. Comput. Appl., vol. 82, pp. 56–64, 2017.

[11]. Wu, L., Wang, J., Zeadally, S. *et al.* Privacy-preserving auditing scheme for shared data in public clouds. *Journal of Supercomputing 74*, pp 6156–6183, 2018.

[12]. Kumar, D. and Smys, S., Enhancing Security Mechanisms for Healthcare Informatics Using Ubiquitous Cloud.

Journal of Ubiquitous Computing and Communication Technologies, 2(1), pp.19-28, 2020.

[13]. Al-Issa, Y., Ottom, M.A. and Tamrawi, A., eHealth cloud security challenges: a survey. Journal of healthcare engineering, 2019.

[14]. Jusak, J., Mahmoud, S.S., Laurens, R., Alsulami, M. and Fang, Q., A New Approach for Secure Cloud-Based Electronic Health Record and its Experimental Tested. IEEE Access, 10, pp.1082-1095, 2021.

[15]. Thakkar, V. and Shah, V., Investigation of Techniques used for Mitigating Security and Privacy Issues in Cloud Based Electronic Health Record (EHR) Systems. vol, 8, pp.466-478, 2021.

[16]. M. Joshi, K. Joshi and T. Finin, Attribute Based Encryption for Secure Access to Cloud Based EHR Systems, *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, 2018, pp. 932-935.

[17] Prasadu Peddi (2015) "A review of the academic achievement of students utilising large-scale data analysis", ISSN: 2057-5688, Vol 7, Issue 1, pp: 28-35

[18] Prasadu Peddi (2015) "A machine learning method intended to predict a student's academic achievement", ISSN: 2366-1313, Vol 1, issue 2, pp:23-37.