IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 7, July 2022

DOI: 10.17148/IJARCCE.2022.11762

ELECTRONIC PERSONAL HEALTH RECORD SHARING SYSTEM

Meghana D S[1], Sowmyashree K M [2]

Research Scholar, Dept. of MCA, P.E.S College of Engineering, Mandya, India[1]

Assistant Professor, Dept. of MCA, P.E.S College of Engineering, Mandya, India[2]

Abstract: For every individual person there personal information or data in the most important in there life. No one likes to share there personal information with the others without the reason. The health data of a person is more confidential because none likes to say that I'm suffering from this disease and so on to avoid the problem of leaking of the personal data this Electronic personal health record sharing system is developed. Where patient can upload there data into the cloud and keep there file safely, in order to secure the data the Key Generator controller and admin works. In this patient can able to perceive the important and vital of security to the private information or info(information) in recent years, the rapid expansion of the web technologies and the lot of net users black net, caused to rapid development of the IOT, which has resulted in the introduction of development of numerous unique applications. The e-health commerce system is one among them, as it can give them advantageous, excellent medical care. In the interim, a critical area of interest and consideration is safeguarding the protection and security of a user(client)'s very own well-being information.

Keywords: Cloud, Secret Keys (special key), Advanced Encryption Standard (AES), Rivest Cipher 4(RC4), Key generator controller.

I. INTRODUCTION

To a person there personal information or data in the most important in there life. No one likes to share there personal information with the others without the reason. The health data of a person is more confidential because none likes to say that I'm suffering from this disease In this perceive the important and vital of security to the private information or info(information) in recent years, which has resulted in the introduction of development of numerous unique applications. The e-health commerce system is one among them, as it can give them advantageous, excellent medical care. In the interim, a critical area of interest and consideration is safeguarding the protection and security of a user(client)'s very own well-being information. There have been other proposed cryptography strategies, such scrambling user(client) information prior to sharing it. Notwithstanding, trading info(information) with a few gatherings (specialists, government assistance, clinical divisions, and so forth) is conceivable infer-able from the need that information be encoded utilizing the extraordinary Secret keys(special key) of every beneficiary. In spite of the fact that there are various limit secret sharing techniques like AES Algorithm and Rivest Cipher 4(RC4) algorithm that might be utilized to move info(information) with only one encryption activity expected, there are a few limitations about the need that the unscrambling secret keys be made by a solitary party.Patient can upload there details to cloud so the file is safe and secured, any unauthorized members can not access or view the details in the file.In this project doctor and superintendent can access view the patient details when the admin allows it and provides the secret keys only then the doctor and superintendent can access the patient details.

II. RELATED WORK

According to the literature survey on this project there are numerous algorithms can be used to generate the secret keys like Secret key cryptography which is also called as symmetric key cryptography the reason is the same single key is used to both decrypt and encrypt the info. Advanced Encryption standard algorithm, Rivest Cipher 4.

1. Utilizing blend hubs and blockchain, a cloud-based secure individual wellbeing record the executives system[2020]
User(client)s of an e-health well-being framework have two fundamental worries: security and protection of patient well-being info(information). Unapproved user(client)s, including outsiders, ought not be ready to interface the papers containing the re-appropriated well-being info(information) to their own info(information) for security reasons. Utilizing blend networks for inconspicuous rethought info(information) access and block-chain for reevaluated info(information) trustworthiness, this paper proposes a mystery keys-based in offer. Based on using Block-chains, a urgent security need known as forward protection is constructed, forestalling an e-medical services supplier from

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 7, July 2022
DOI: 10.17148/IJARCCE.2022.11762

getting to any future well-being records after her meeting has finished. It is recommended and inspected how to distribute and get to clinical records.

2.Secure Management System For Electronic Health Record (2020)

The "Got Electronic Health Record Management System's" venture will probably safeguard the info(information) set holding the patient's singular clinical and medical clinic records. The current framework, which is very much kept up with by medical services suppliers, disapproves of keeping up with patient records. They are frequently kept up with physically, and most of the patient information base or history is challenging for specialists to get to.

This affects the norm of patient consideration, as it brings about additional successive solutions or tests, greater expenses, and longer treatment times. It is only excessively straightforward for somebody with malevolent plan to get into frameworks, take classified information, and use it against others. An exceptionally solid and safe info(information) set is fundamental, particularly when it houses touchy info(information). Patients may not report their actual clinical issue in view of worry for the classification and protection of their well being related information. With the main sideways reason for bringing down the time and assets required for comparative positions like this, this undertaking supports taking care of the mentioned issue in a more compelling and cost-logical way so the important institutional assets might be used with completion of success. This drive means to shield patient well being info(information) from programmers and assailants.

3. Cloud-based PHR the chiefs that is mixed and uses the DES plan [2021]

Systems for administering patient individual prosperity records that are arranged in the cloud are called cloud-based patient prosperity record structures (CB-PHR). Consistent, adroit exchange of clinical consideration info(information) is made possible by circulated processing. The fundamental blocks to the unlimited gathering of CB-PHR structures are info(information) security and assurance of staying aware of patient prosperity record systems. Since prosperity information is very sensitive, it ought to be stayed aware of in an extraordinarily gotten way. Considering the difficulties and different security endeavors in the continuous structure, this study proposes an exceptional system for continuing prosperity records utilizing the info(information) Encryption Standard (DES) in offer. Documents are mixed including going against secret keys in this methodology, and the encoded information records from various information sources may be joined. Also, it offers a simple to-utilize, security defensive inquiry component with only one information demand from the information purchaser. Cloud will refine scrambled information from all incidental information sources without uncovering the inquiry's substance.

4. Patient health record system in KRS Hospital Mysore

The patient details are uploaded by the registration member or the authorized persons only, the details can only be accessed by using the ip-address so they can view the patient name date of admission and the cause of the disorder(or sickness). This information can only be accessed by the administer doctor or patient can not access this and also patient cannot upload the information.

III. METHODOLOGY

Cloud is the platform where the data or the file of an individual is stored. By using AES algorithm the secret key is generated for the login by verifying the details, and by using the secret key shared by Key generator controller to the users mail where users are doctor or the superintendent. The users login informations are stored in the database which can be view-able by the admin. Admin can view the analysis chart, info of the users.

A. Database:

All the users information is stored in the database which is connected to the project using the libraries like JDBC and ODBC. Users info like id, password,age,DOB and other basic information are stored.

B. Normalization:

2NF is used in this because there will be doctors or superintendent of the same name but there id will be differ or the other entity entered will be differ and the foreign key is the password used to register which is used as the foreign key while login .

C. System Architecture:

We can understand the basic flow of the project where patient acts as the owner and doctor or superintendent acts as users and KGC is the key generator controller and medical server is the admin of this system.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 7, July 2022

DOI: 10.17148/IJARCCE.2022.11762

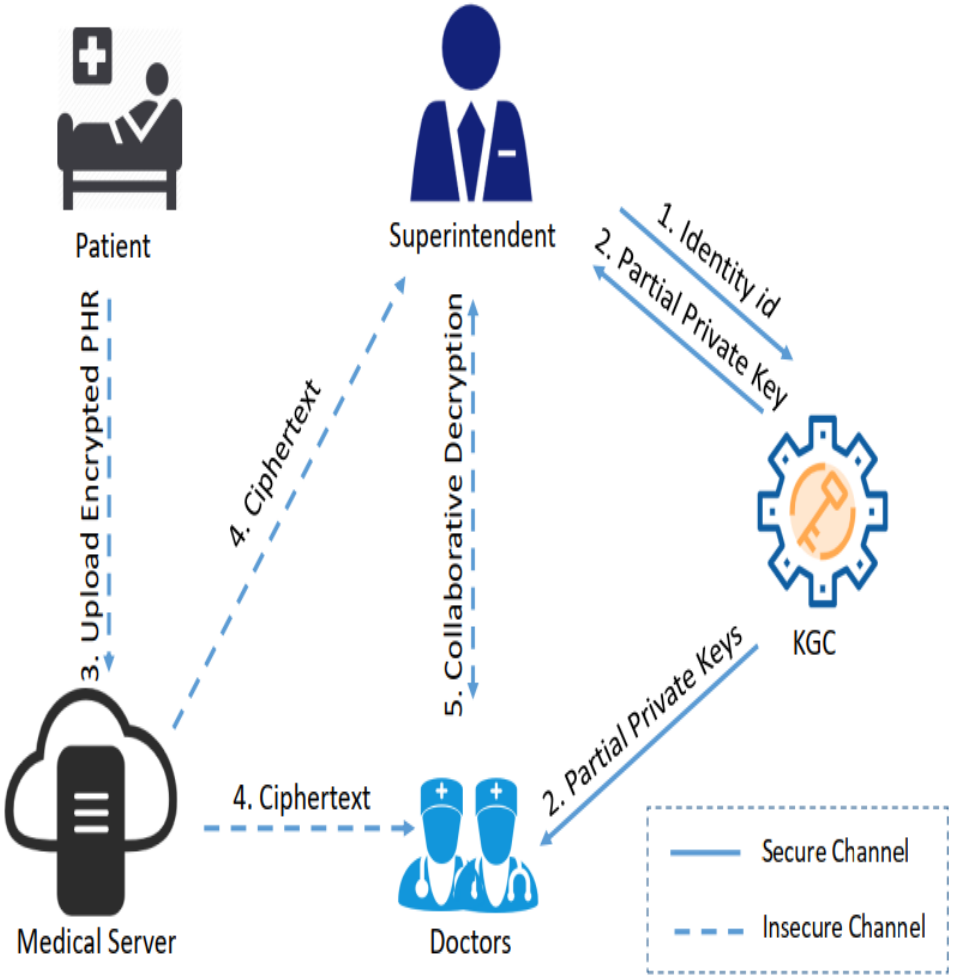


Figure 1 System architecture for Hand Gesture

IV. IMPLEMENTATION

The e-health commerce system is one among them, as it can give them advantageous, excellent medical care. In the interim, a critical area of interest and consideration is safeguarding the protection and security of a user(client)'s very own well-being information. There have been other proposed cryptography strategies, such scrambling user(client) information prior to sharing it. Notwithstanding, trading info(information) with a few gatherings (specialists, government assistance, clinical divisions, and so forth) is conceivable infer-able from the need that information be encoded utilizing the extraordinary Secret keys(special key) of every beneficiary. In spite of the fact that there are various limit secret sharing techniques like AES Algorithm and Rivest Cipher 4(RC4) algorithm that might be utilized to move info(information) with only one encryption activity expected, there are a few limitations about the need that the unscrambling secret keys be made by a solitary party.Patient can upload there details to cloud so the file is safe and secured, any unauthorized members can not access or view the details in the file.In this project doctor and superintendent can access view the patient details when the admin allows it and provides the secret keys only then the doctor and superintendent can access the patient details.

Cloud is the platform where the data or the file of an individual is stored. By using AES algorithm the secret key is generated for the login by verifying the details, and by using the secret key shared by Key generator controller to the users mail where users are doctor or the superintendent. The users login informations are stored in the database which can be view-able by the admin. Admin can view the analysis chart, info of the users.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 7, July 2022

DOI: 10.17148/IJARCCE.2022.11762

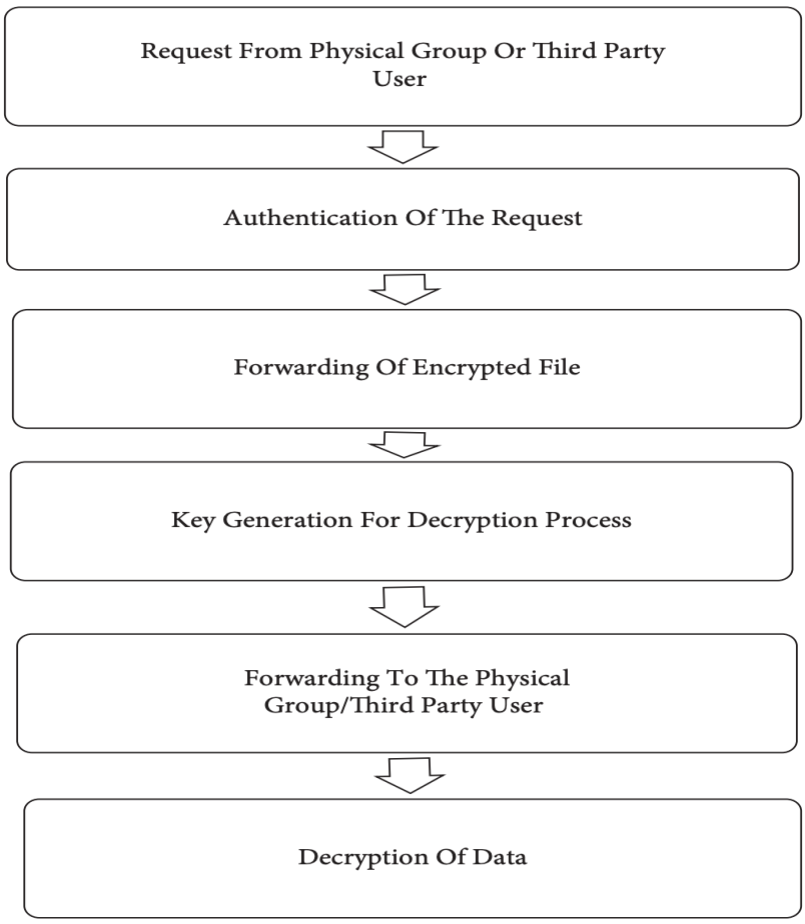


Figure 2 Flow of implementation

V. CONCLUSION

In this project the main agenda is to protect and secure the patient health record.

1. Patient can upload the file to cloud and view the uploaded file
2. Doctor and superintendent can request to view the file.
3. KGC approve the Doctor and superintendent register by providing the secret keys
4. Admin can view all the users details and approves the request to view the file, Admin can also view the analysis by this he/she can understand how many users are using the applications.

VI. FUTURE ENHANCEMENT

1. Can look into some more efficient techniques in the future, such as removing the zero-knowledge proof from the scheme and distributing the secret without requiring a secret channel.
2. Adding feedback so that doctor can easily provide precautions to be taken.
3. Adding chat facility so the doctor or patient can contact each other without contact info.
4. Making the file accessible for the authorized doctor so that he can also view the file,only the patient can approve that request.

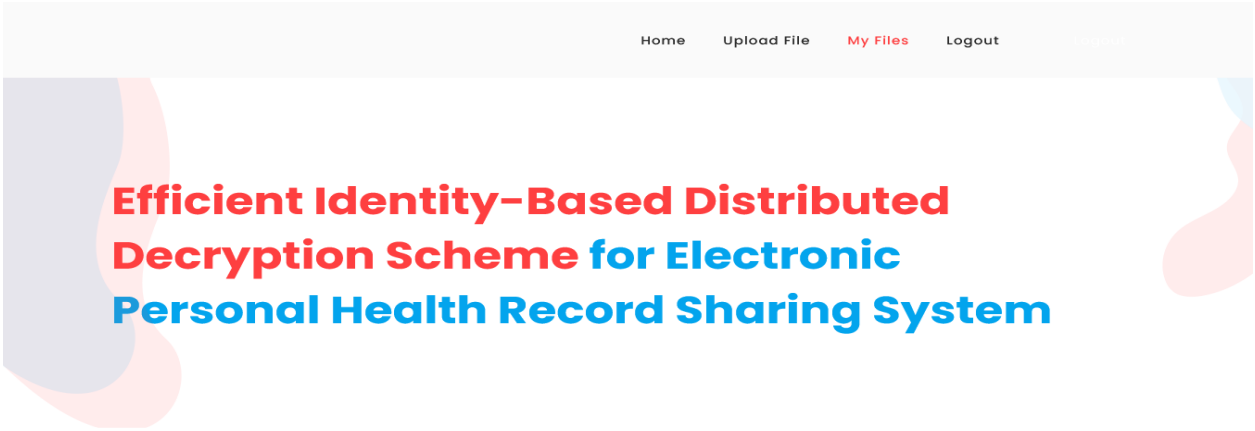
IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 7, July 2022

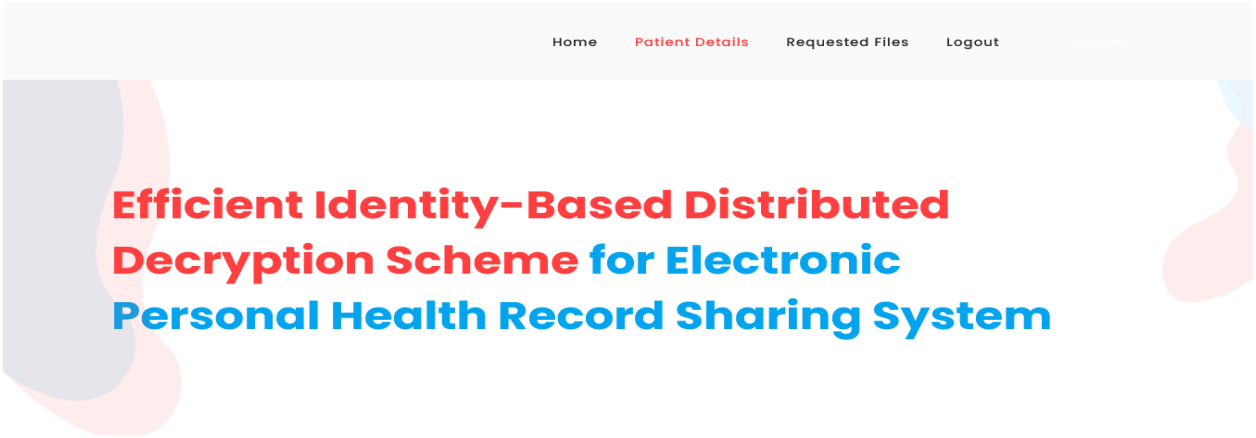
DOI: 10.17148/IJARCCE.2022.11762

VII. OUTPUT SCREENSHOT



My Files

User Name	File ID	File Name	Uploaded Time	D Key
abdul	1	test.txt	2021/06/29 20:08:33	xsyhsdmMN+lAk69n1d4VJw==



Encrypted Patient Details

Name	Age	Blood Group	Occupation	Height	Weight	Bl
abdul	8s9ZAcLRnEE=	wUdGbNw5qtA=	HBomEowFOk9ZC5AMfleObw==	e0mRzeUFK9E=	OmgGj/N2jHY=	17

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 7, July 2022

DOI: 10.17148/IJARCCE.2022.11762

REFERENCES

[1] G. Eysenbach, "What is e-health?" J. Med. Internet Res., vol. 3, no. 2, p. e20, 2001.

[2] V. Chang, Y.-H. Kuo, and M. Ramachandran, "Cloud computing adoption framework: A security framework for business clouds," Future Gener. Comput. Syst., vol. 57, pp. 24–41, Apr. 2016.

[3] M. Obaidat and N. Boudriga, Security of E-Systems and Computer Networks. Cambridge, U.K.: Cambridge Univ. Press, 2007.

[4] P. C. Tang, J. S. Ash, D. W. Bates, J. M. Overhage, and D. Z. Sands, "Personal health records: Definitions, benefits, and strategies for overcoming barriers to adoption," J. Amer. Med. Inform. Assoc., vol. 13, no. 2, pp. 121–126, Mar. 2006.

[5] R. Pifer. Patient Use of Digital Health Tools Lags Behind Hype, Poll Finds. Accessed: Sep. 12, 2019. [Online]. Available: https://www.healthcaredive.com/news/patient-use-of-digital-health-tools-lags-behindhype-poll-finds/5627 78/

[6] Protenus. (2018). 32 Million Breached Patient Records in First Half of 2019 Double Total for all of 2018. Accessed: Jul. 31, 2019. [Online]. Available: https://www.prnewswire.com/news-releases/32-million-breached-patient-records-in-first-half -of-2019-double-total-forall-of-2018-300894237.html

[7] J. L. Fernández-Alemán, I. C. Señor, P. Á. O. Lozoya, and A. Toval, "Security and privacy in electronic health records: A systematic literature review," J. Biomed. Informat., vol. 46, no. 3, pp. 541–562.