International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 05 | May - 2022 Impact Factor: 7.185 ISSN: 2582-3930

SECURE SHARING OF PHR USING ECC

V.Nanda kumar [1],Ajay R[1], Gokulnath S J[1], Hrithik Baarathi T[1], Joel Antony Shravan J [1]

[1] Students - Department of Computer Science Engineering

[*1] Assistant Professor, Department of Computer Science Engineering,

PSNA College of Engineering and Technology, Dindigul - 624005, Tamil Nadu, India

Abstract - Electronic health records possess the patient's medication details and their health history. The health records attract the attention of the attackers' as it possesses invaluable information. Loss of electronic health record leads to a wrong medication or surgery. PHR generally contains highly-sensitive and critical data related to patients, which is frequently shared among clinicians, radiologists, healthcare providers, pharmacists, and researchers, for effective diagnosis and treatment. Key exchange protocols enable two or more parties to establish a shared encryption key that they can use to encrypt or sign data that they plan to exchange. As key exchange schemes with certificates require some trusted authority to verify integrity of the received messages, the extension to a larger system may be difficult. They need a large storage for certificates and more bandwidth for the verification of the signature as the number of user's increases. The authentication method requires that the client and server are each pre-provisioned with a unique asymmetric Elliptic Curve Cryptography (ECC).

Keywords – Personal Health Record(PHR),ECC

I.INTRODUCTION

- The widespread acceptance of cloud based services in the healthcare sector has resulted in cost effective and convenient exchange of Personal Health Records (PHRs) among several participating entities of the e-Health systems. Storing the confidential health information to cloud servers is susceptible to revelation or theft and calls for the development of methodologies that ensure the privacy of the PHRs.

- PHR generally contains highly-sensitive and critical data related to patients, which is frequently shared among clinicians, radiologists, healthcare providers, pharmacists, and researchers, for effective diagnosis and treatment. Key exchange protocols enable two or more parties to establish a shared encryption key that they can use to encrypt or sign data that they plan to exchange. The authentication method requires

that the client and server are each pre-provisioned with a unique asymmetric Elliptic Curve Cryptography (ECC).

- The PHR owners should be able to store the encrypted data on the cloud and only the authorized users possessing valid re-encryption keys issued by a semi trusted proxy are able to decrypt the PHRs.

II.MODULES

- **Authentication Framework:**

Admin should create secure EHR sharing framework.The security of the communication between doctors and the intermediate server is based on a Session based Authentication and a Key Exchange (AKE) scheme that provides mutual authentication between doctors and the admin through a control unit. Then create control unit that used for verification process. Set security parameters and key generation functions.

- **User Enrolment:**

User enrolment is the process of registering with application to make communications. Here users are defined as doctor and admin. Both are registered in this application and get authentication keys for login process. For registering process, they should enter the details like name, father name, gender, age, mobile number, email id, username and password. Registered details are sending to the control unit for confirmation.

- **Key Distribution:**

Key distribution is the process of generating secret keys and distributing the keys to the registered users. Control unit take responsible for key generation and distribution process. In proposed work, ECC based key generation scheme has been implemented. Then the keys will be sharing to the registered users through their mail id. The Elliptic Curve Cryptography (ECC) is one of the most efficient algorithms for securing data. The Authenticated Key Agreement (AKA) protocol is used for establishing a common session key between the two communicating parties. Authenticated key agreements enable users to

determine session keys, and to securely communicate with others over an insecure channel via the session keys.

- **PHR Sharing:**

This module explains about PHR sharing by admin. Admin should authenticated by control unit using username, password and secret key. The entered details are validated by control unit. Then they will be allowed to share medical information to the patients. . This proposed work investigates the lower bounds on

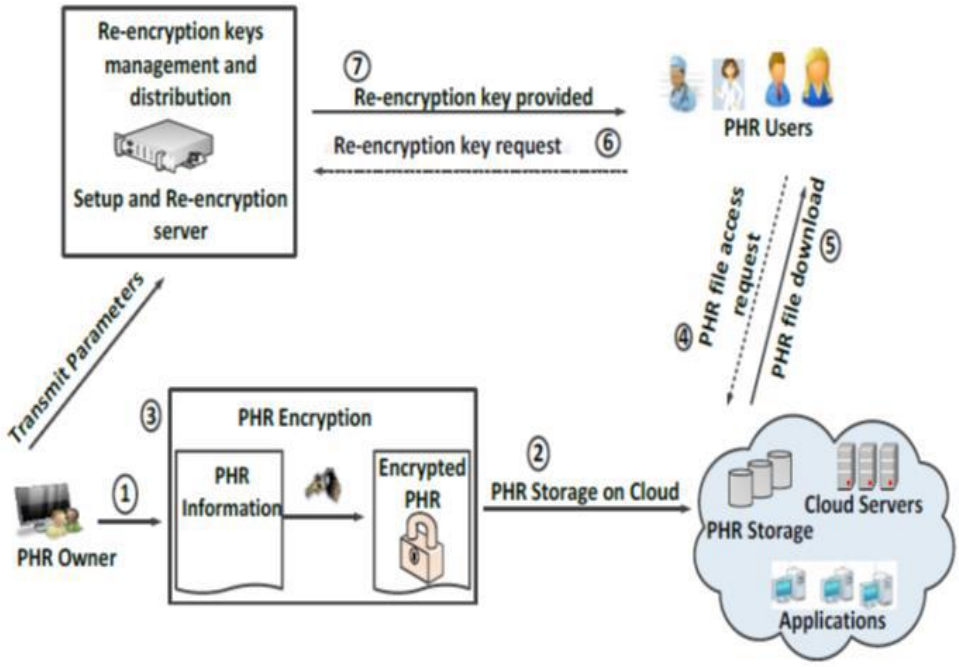
communications for two-party authenticated key agreements and considers whether or not the sub-keys for generating a session key can be revealed in the channel. Since two clients do not share any common secret key, they require the help of the control unit to authenticate their identities and exchange confidential and authenticated information over insecure networks.

- **Key and Session Verification:**

In this module data access process has been explained. Data access is the process of accessing shared PHR by admin. Before accessing PHR, Doctors should authenticated using their username, password and login key. After that doctors session time will be checking by the system. When all details entered by the doctors are correct including the session time, then they will be allowing accessing PHR from proposed framework. If the session time gets lost, they will be send request to the admin to share new key permission.

III.ARCHITECTURE:

- **Basic Block Diagram.**



IV.RELATED WORKS

1. Author: J. Pecarina, S. Pu, and J.-C. Liu.
Year: 2011
Title: "SAPPHIRE: Anonymity for enhanced control and private collaboration in healthcare clouds".

2. Author: C. Leng, H. Yu, J.Wang, and J. Huang.
Year: 2013
Title: "Securing personal health records in the cloud by enforcing sticky policies".

3. Author: Mazhar Ali, Assad Abbas, Muhammad Usman Shahid Khan and Samee U. Khan.
Year: 2021
Title: "SeSPHR- A Methodology for Secure Sharing of Personal Health Records in the Cloud"

V.EXISTING SYSTEM

There are certain features limiting the process of the present system. In the existing

system,encryption is done using El-Gamal Encryption algorithm.There are various drawbacks present in the technique like its need for randomness, and its slower speed (especially for signing). Another potential disadvantage of the El Gamal system is that message expansion by a factor of two takes place during encryption (means the cipher text is twice as long as the plaintext).Other systems are dependent on the Cloud Service Provider for encryption which may lead to data leakages .Some systems require the PHR owner to be online fulltime which may cause inconveniences.

VI.MERITS OF THE PROJECT

1. Very fast key generation.
2. Smaller keys, cipher-texts, and signatures.
3. Fast signatures.
4.. Moderately fast encryption and decryption.
5. Right protocols for authenticated key exchange.

VII.REQUIREMENTS

- **Hardware Requirements**

Processor	:	Intel(R) Core (TM) i3
Processor Speed	:	3.06 GHz
Ram	:	4 GB
Hard Disk Drive	:	250 GB

- **Software Requirements**

Language Used : ASP.net
Algorithm U sed : Ellyptic Curve Cryptography
IDE : Visual Studio Code
Database : My SQL

VIII.TESTCASE

S.NO	FUNCTION	DESCRIPTION	EXPECTED OUTPUT	ACTUAL OUTPUT	STATUS
1	Authentication Framework	GUI for each users	Web pages are created	Web pages are created	Success
2	User Enrolment	User register and get approval	User login to the system	User login to the system	Success
3	Key Distribution	File upload and encrypted	Encrypted files	Encrypted files	Success
4	PHR Sharing	Share to the other users	Key sent in email	Key sent in email	Success
5	Key and Session Verification	Verify the decrypt key with time	Decrypt the files	Decrypt the files	Success

IX.CONCLUSION:

We proposed a methodology to securely store and transmission of the PHRs to the authorized entities in the cloud.
The methodology preserves the confidentiality of the PHRs and enforces a patient-centric access control to different portions of the PHRs based on the access provided by the patients.