NOVEL ARCHITECTURE FOR SECURING HEALTHCARE INFORMATION

Prof. A.G Said[1], Abhishek Rastogi[2], Nupur Pandey[3],Krishna Shelke [4]

[1,2,3,4]Department of Computer Engineering

[1,2,3,4]AISSMS's Institute of Information Technology, Pune, India

***Abstract* —** Secure Healthcare Network provides a secure platform for the patients to share their medical documents over the cloud in a more effective way. Providing security to the data has been the major issue while sharing data over the cloud services. In this paper, we will provide patients with a platform where they can interact with doctors without having any concerns about someone accessing their data without their knowledge. We will encrypt the data provided by the patients in a way that it is not accessed by others. For doing so, we will convert their data into binary data and then that data is divided into block of 128 bit which will be encrypted and for each block a key will be generated. The secured data will be accessed by the doctors shortlisted by the system and selected by the patients. Suggesting of doctors is done by the system after reading a document which is made mandatory while uploading the data which will help the system to recognize the symptoms of the disease from which our system will suggest the list of doctors with whom patient can share their data and give access to. Sharing and storing of documents will be done over the cloud that is why we need to secure our data from hackers etc. If doctors encounter any issue then they can consult specialists then re-encryption would be done so that data of patient is still secure. For the purpose of encryption and decryption we using trapdoor algorithm as our base algorithm. Secure Healthcare Network will turn out to be a time saving platform for both the doctors and patients.

Keywords— Encryption, Re-encryption, Data Security, Management.

I. INTRODUCTION

Healthcare is a modern mixture of technology on the way to offer necessary fitness statistics with the aid of the use of Healthcare gadget, the Digital Health Document of patients can be transmitted over the cloud for storage. Our system is created for connecting sufferers to the doctors so that they could be provided with good advice. With the use of this system, we can interact with doctors and specialists that too without letting anyone exploiting their medical records.

Security of patient's documents is assured by securing the data using encryption method and decryption method which would be done using algorithms which would help us secure our platform from various threats. This would help patients to get their data secured and shared without being illegally accessed. This system would require a mandatory document from the patients along with the medical files which would mention about the symptoms. The system would read this document and after reading the document it would suggest most appropriate doctors to the patients according to the symptoms which would result in best consultation from doctors to patients and better treatment of the disease. This system would help in saving patient's time and travelling cost. Once the doctors are suggested to the patient by the system, it would be in patient's hand to choose the doctor which he/she would prefer. The legal doctors can access the encrypted information of patient placing end to the misuse of patient's essential records.

II. LITERATURE SURVEY

Personal health record (PHR) is an emerging patient-centric model of health information exchange, which is often

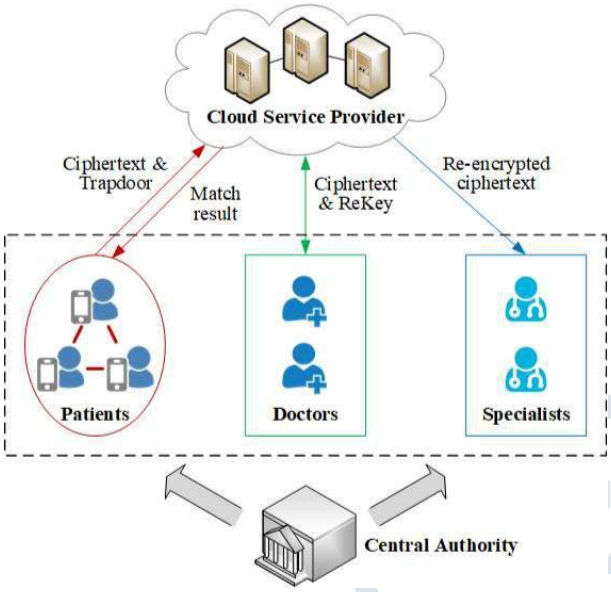
outsourced to be stored at a third party, such as cloud providers. However, there have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties. To assure the patients' control over access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing.

The problem of patient self-controlled access privilege to highly sensitive Personal Health Information (PHI), where PHI is expected to be securely stored in cloud storage for uninterrupted anytime, anywhere remote access. In order to assure the privacy of PHI, we propose Efficient and Secure Patient-centric Access Control (ESPAC) scheme which allows data requesters to have different access privileges based on their roles, and then assigns different attribute sets to them

Making new connections according to personal preferences is a crucial service in mobile social networking, where the initiating user can find matching users within physical proximity of him/her. In existing systems for such services, usually all the users directly publish their complete profiles for others to search. However, in many applications, the users' personal profiles may contain sensitive information that they do not want to make public.

Conditional proxy re-encryption (CPRE) enables fine-grained delegation of decryption rights, and has many real-world applications. In this paper, we present a ciphertext-policy attribute based CPRE scheme, together with a formalization of the primitive and its security analysis. We demonstrate the utility of the scheme in a cloud deployment, which achieves fine-grained data sharing.

III. SYSTEM ARCHITECTURE



IV. PROPOSED METHODOLOGY

Key with variable length (128,192, 256 bit)

Represented with a matrix {array) of bytes with 4 rows and Nk columns, Nk=key length / 32

key of 128 bits= 16 bytes 7 Nk=4

key of 192 bits= 24 bytes 7 Nk=6

key of 256 bits= 32 bytes 7 Nk=8

$K_{0,0}$	$K_{0,1}$	$K_{0,2}$	$K_{0,3}$
$K_{1,0}$	$K_{1,1}$	$K_{1,2}$	$K_{1,3}$
$K_{2,0}$	$K_{2,1}$	$K_{2,2}$	$K_{2,3}$
$K_{3,0}$	$K_{3,1}$	$K_{3,2}$	$K_{3,3}$

Block of length 128 bits=16 bytes

Represented with a matrix(array) of bytes with 4 rows and Nb Columns ,Nb=block length/32

Block of 128 bits= 16 bytes 7 Nb=4

in_0	in_4	in_8	in_{12}
in_1	in_5	in_9	in_{13}
in_2	in_6	in_{10}	in_{14}
in_3	in_7	in_{11}	in_{15}

Internally, the AES's algorithm operations are performed on the two-dimensional array of bytes called state

- 4 rows, each containing Nb bytes
- Nb columns, constituted by 32-bit words
- Sr,c denotes the byte in row r and column c

The array of bytes in input is copied in the state matrix

$$S_{r,c} \leftarrow in$$

At the end the state matrix is copied into the output matrix

$$out \leftarrow S_{r,c}$$

- Operations performed on state(4 rows of bytes).
- The 128 bit key is expanded as an array of 44 entries of 32 bits words,4 distinct words are serves as a round key

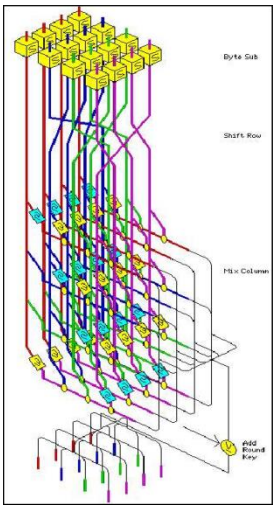
For each round, key schedule lies on the S-box

State = x;

1. Add roundkey(State, key0)
2.for r=1 to (Nr-1)
   - SubBytes(State ,S-box)
   - Shiftrows(State)
   - Addround key(State , keyr)

1. SubBytes(State,S-box)
2. Shiftrows(State)
3. Addround key(State, keynr)

Y =State



V. APPLICATION

1. To detect malicious activity and stop attacks.

2. Healthcare organizations are required to maintain compliance across a vast landscape of providers, doctors, administrators and multiple devices including desktops, laptops, tablets and smart phones. Transferring sensitive and private information, known as electronic protected health information.

3. Secure information access and sharing is a fundamental requirement for the legal profession. Shared case information is proprietary, privileged, and sensitive.

4. Financial institutions face security threats daily. Today's bank robber wears multiple masks: identity thief, hacker, and online, check, mail, and card fraudster.

5. Securing the nation's transportation and shipping infrastructure against disasters, terrorism, and other security threats demands the highest enterprise data security platform to efficiently share sensitive information and files in scheduled, ad hoc, and emergency situations.

VI. CONCLUSION

Provide secure system for sharing of medical data of patients over the cloud and suggesting list of doctors to patients automatically by reading the symptoms from the mandatory document .The analysis and results show that the computation cost on patient side is reduced.

REFERENCES

[1] M. Li, S. Yu, Y. Zheng, K. Ren and W. Lou, Scalable and secure sharing of personal health records in cloud computing using attribute- based encryption, IEEE Trans on Parallel and Distrib. Syst., vol. 24, no. 1, pp. 131-143, Jan. 2013.

[2] M. Barua X. Liang, R. Lu and X. Shen, ESPAC: Enabling Security and Patient-centric Access Control for eHealth in cloud computing, International Journal of Security and Networks, vol. 6, no. 2/3, pp. 67-76, Nov. 2011.

[3] T. Matsuo, Proxy re-encryption systems for identity-based encryption, in Proc. 1st International Conference on Pairing-Based Cryptography, Tokyo, Japan, 2007, pp. 247-267.

[4] Y. Zhou, H. Deng, Q. Wu, B. Qin, J. Liu and Y. Ding, Identity-based proxy re-encryption version 2: Making mobile access easy in cloud, Future Generat. Comput. Syst., vol. 62, pp. 128-139, Sept. 2016.

[5] M. Li, N. Cao, S. Yu and W. Lou, FindU: Privacy-preserving personal pro_le matching in mobile social networks, in Proc. 2011 IEEE Inter- national Conference on Computer Communications, Shanghai, China, 2011, pp. 2435-2443.

[6] Y. Yang, H. Zhu, H. Lu, J. Weng, Y. Zhang and K. Choo, Cloud based data sharing with _ne-grained proxy re-encryption, Pervasive and Mobile Computing, vol. 28, pp. 122-134, Jun. 2016.

[7] L. Zhang, X. Li, K. Liu, T. Jung and Y. Liu, Message in a sealed bottle: Privacy preserving friending in mobile social networks, IEEE Trans. Mob. Comput., vol. 14, no. 9, pp. 1888-1902, Sept. 2015.

[8] S. Ma, Identity-based encryption with outsourced equality test in cloud computing, Information Sciences, vol. 328, pp. 389-402, Jan. 2016.