Id Based Health Care System

Nikita Deulkar, Nikita Bhandare[2], Komal Waghmare[3], and Pratik Kamble[4], Prof Ashish Gaigol[5]
[1, 2, 3, 4] Savitribai Phule Pune University

Abstract- *Sharing of health information become daily routines in which hospitals and clinics often refer patients to specialists because of their limited facilities, services, and number of specialist physicians. This paper proposed secure design for sharing referral medical record using HIBE (Hierarchical ID Based Encryption), that focused on the ability of sharing information and ensuring privacy of referral medical record. Our proposed system is able to secure referral medical record from third parties and only the referral physician that can access the referral medical record.*

Keywords- health information; sharing; privacy; referral medical record;

I. INTRODUCTION

Your Health ID is created by using your basic details and Mobile Number or Aadhaar Number. Thus, it will be unique to you and you have the option to link all your health records to this ID. You can also choose to create multiple IDs as modules for storing different segments although it is preferred and recommended that Health ID.

Any Public Hospital, Community Health Centre, Health and Wellness Centre across India or any Healthcare provider who is in the National Health Infrastructure Registry will be able to support you to obtain a Health ID. You can also obtain a Health ID by self-registration. You can register here h Name,Year of Birth, Gender, Mobile No./Email, Aadhaar (optional) No. The process of generation of Health ID has voluntary usage of AADHAAR. This shall require a notification under Section 4 of AADHAAR Act. In addition, all Government financed health benefit schemes that require mandatory use of Aadhaar will have to notifiy under Section 7 of AADHAAR Act \ The idea for a health ID was first floated in 2017, when the government proposed creating a digital health system that would integrate information for citizens and stakeholders across private and public healthcare providers. It is expected that hospitals, online pharmacies, telemedicine firms, laboratories and insurance companies will take part in the new system.Additionally it is hoped the digital health ID will reduce preventable errors and improve quality of care, while making it possible for users to easily view their own medical records.

Main motivation of our project that personal data will be protected, and will only be shared with medical professionals once the user has given their consent, who remains the owner of the records.

While the initiative has been widely welcomed, experts have emphasised that the privacy of people’s health data is vital. Measures to safeguard this include blockchain technology to ensure records are encrypted, consent when accessing and storing records, anonymising personal data and ensuring data stored in the cloud is secure from hackers

A. Definitions

Some of the definitions used in this method include[9-10]: ID. The position of user at each hierarchy is defined by series : (, … ,). The highest position in the hierarchy is PKG, while the lower positions are marked by the user with series {(, … ,): 1 ≤ < }.

Root Setup. Root PKG takes security parameter and return system parameter and secret root. System parameter contains message space and cipher text space . System parameter can be known by all users while root secret is confidential and only be known by PKG.

Lower Level Setup. Lower level from root PKG should take system parameter and generate private key for their children. Extract. Root PKG and lower level with series of (, … ,) can generate private key for their children by using their own system parameter and private key.

Encrypt. Sender inputs M where and series of ID for each message, thus generate cipher text ∈ . Decrypt. Recipient input ∈ and private key d, and message M will be obtained.

B. Hierarchical ID-Based Encryption Schemes (HIBE) Let be the set of entities at level i, where = { }. Root Setup. Root PKG: 1. Run on input K to generate group , from order prime q and pairing (1) where parameter is Bilinear Diffe-helman (BDH) generator. ê: × → (1) 2. Select generator ∈.
3. Select random value ∈ /q and set= ;
4. Select : {0,1}∗ → as cryptographic hash function and : → {0,1} for some n, where and treated as random oracles. Let = {0,1} be the message space, and cipher text space = x {0,1}

meanwhile t is level of recipient. System parameter is (,, ê,,,,) and ∈ /q is secret from root PKG.

Lower Level Setup. Let ∈ be entity, and select a random value ∈ /q . Extract. Let E be the entity at Level by series ID (ID,..., ID), where (ID,...,ID) for 1 ≤ i ≤ t. Set as identity element of . 1. Generate (2) = (ID,..., ID) ∈ (2) 2. Set private key (3) = + =∑ (3) 3. Get value of = for 1 ≤ i ≤ t − 1

Encrypt. Sender: 1. Calculate value of = (ID,..., ID) ∈ for 1 ≤ i ≤ t. 2. Select Random value of r ∈ /q . 3. Set cipher text (4) where =῀(,) C = [r, r,…, r, M ⊕()] (4)

Decrypt. For decrypt cipher text C=[,,…,,V] ∈ C, calculate message M (5) = ⊕ ῀(,) ∏ˆ(, (5) Remark 1. Each has secret value ∈ /q like root PKG. use secret value to generate secret point for each child. Each lower level PKG do not always use the same to extract each private key.

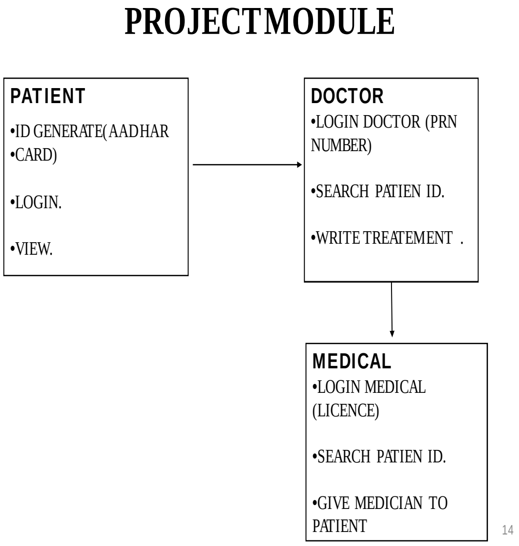
Remark 2. can be selected become hash function iteration, so can be calculated as (,). Remark 3. is private point from and {: 1 ≤ < } is value of Q from . and : 1 ≤ < is valid private key for (, … ,) if = + ∑ and = for (, … ,) ∈ (/).

II. SECURE SHARING REFERRAL MEDICAL RECORD SYSTEM DESIGN

We propose design of secure sharing referral medical record system and guarantee of medical records privacy. This model is critical issue in providing service with higher level confidence (trust) to client. 2016 2nd International Conference on Science in Information Technology (ICSITech) 233

A. Entity and Definitions Entities

that involved in this sharing system are patient, referring physician, referral physician, storage server and public storage server as shown in Fig. 1. Patient is a person who would be protected his medical records. In the data sharing procedures, physician who shares patient's referral medical record called as referring physician, and physician who receive patient's referral medical record called as referral physician. Storage server located at each hospital and serves to store medical records. Public storage server is located in the public health office and serves to store medical records of patients who had been referred that called as referral medical record. This medical record is part of EHR. Fig. 1



1. Entities in EHR Sharing System

B. Security Requirements Sharing System must be fulfilled security requirements as follows:

Privacy. Sharing system achieve privacy if patient's referral medical records can only be accessed by authorized physicians for legitimate reasons. Authentication.

Authenticity shows that each entity involved in the sharing system must be managed to authenticate or verify the identity of each other, even if it is cross domain authentication.

Confidentiality. Confidentiality requires that the contents of the medical record could not be learned by the attacker, which basically ensures the privacy of patients as determined in terms of privacy.

Integrity. The system ensures that medical record that saved is not modified except by authorized physician in accordance with the consent or request of the patient. In addition, the message exchange protocol will not be modified by a malicious party.

C Secure Sharing Referral Medical Record System

Design First level of health-care (hospitals) often refer patients to second level of health-care (specialist) if they need further care or inability first level of health-care to provide health services in accordance with the needs of patients because of limited facilities, services, or number of specialist physicians. This system is one kind of hierarchy that allows the trust problem of patient at referral cases, because there must be medical record's sharing between first level of health care to second level of health care.

D. Generate of Key Protocol.

In this research, we use HIBE method for cross-domain authentication. Public health office acts as PKG (public key generator) that will generate system parameters and secret root. Lower level user (hospital, clinic) should take the system parameters and perform the extraction process to generate public key and secret key that will be used for encryption and decryption process.

E. Referral Protocol.

At referral case the patient will be given card and referral letter as shown in Fig. 2.

Update smart card contains system parameters, private key, and id referral physician, while referral letter equipped with physician's signature and stamp of the hospital. When they arrived at the referral hospital, patient will submit the referral letter to the receptionist. Referral card given to the referral physician and used for accessing referral medical record. EHR in public storage server can be accessed if the referral data from medical records were not sufficient to do proper medical action as shown in Fig. 3. Fig. 2. Referral protocol in referring hospital (Hospital A) F

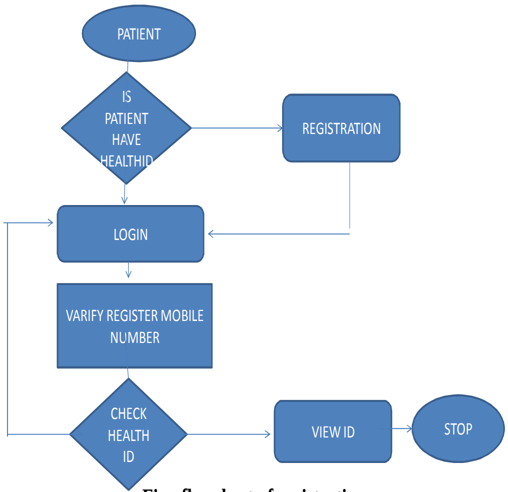


Fig : flowchart of registration process

Fig. 3. Referral protocol in referral hospital (Hospital

III. PROTOTYPE IMPLEMENTATION AND SHARING SYSTEM TESTING

In this section, we demonstrate the prototype implementation and experimental results of our proposed sharing scheme in a desktop PC. The specification of PC is shown in Table

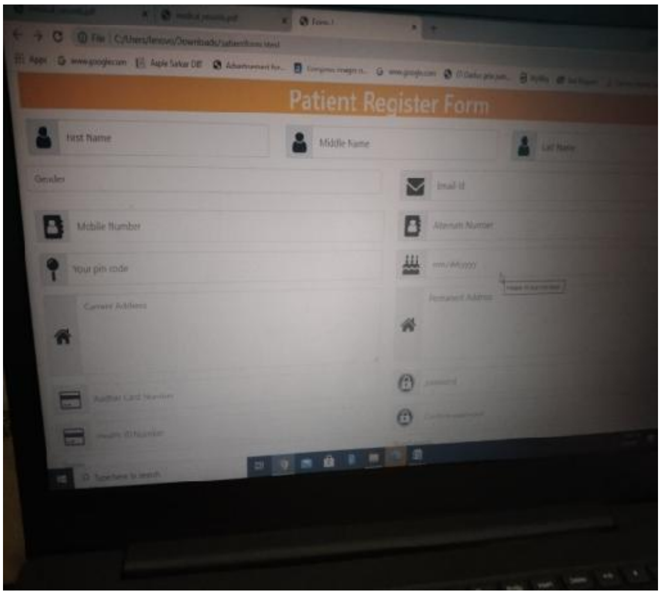
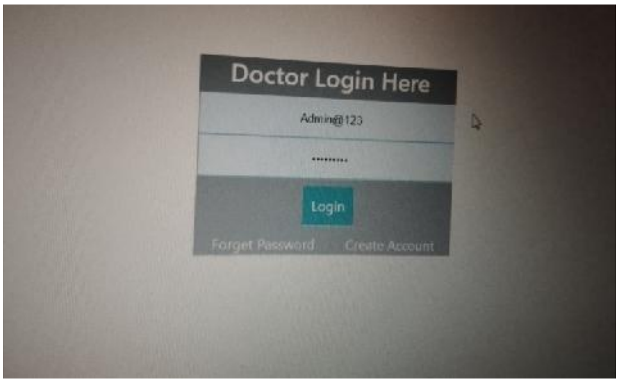


TABLE I. SPECIFICATION OF H/W USED IN EXPERIMENT

Specification of	Remarks
O/S	Windows 10 Home
CPU	Varian prosesor Intel® Prosesor Core™ i5 6200U
RAM	4GB

I. HIBE Testing. HIBE Algorithm has successfully made to encrypt and decrypt referral medical record. Fig. 4 shows the success of generation system parameters and root secret. Fig. 5 shows the extraction process and Fig.6 shows the encryption and decryption process. Fig. 4. System parameter and root secret Fig. 5. Extraction result Fig. 6. Encryption and decryption process Sharing System Testing. Several Testing conducted to determine whether the sharing system has fulfilled security requirement and privacy. Fig. 7 shows the login process to verify the identity of each user. If the verification failed as shown in Fig. 8, User could not access the information on the sharing system. Information that can be accessed depended on the privileges of each user. It shows that the system made has fulfilled authentication and integrity as security requirements because the information only accessed by legitimate user. Fig. 7. Login form F



Doctor Login Here

Admin@123

....

In case of referral, patients will be given referral letter and smart card which contains system parameters, private key, and physician referral id. Fig. 9 shows the referral medical record form that contains the patient's condition, and Fig. 10 shows the referral medical record database

IV. CONCLUSION

Our proposed system is able to secure referral medical record from third parties and only the referral physician that can access the referral medical record. System also already fulfilled 4 security requirements, namely privacy, authenticity, confidentiality and integrity.

V. ACKNOWLEDGMENT

This research was supported by Ministry of Research, Technology, and Higher Education of Indonesia, Hibah Bersaing Scheme 2016. REFERENC

REFERENCES

[1] N. Patel, "Internet of things in healthcare: applications, benefits, and challenges." Internet: https://www.peerbits.com/blog/internet-of things-healthcare-applications-benefits-and-challenges.html

[2] H. Bauer, M. Patel, J. Veira, "The Internet of Things: sizing up the opportunity." Internet: https://www.mckinsey.com/industries/semiconductors/our insights/the-internet-of-things-sizing-up-the-opportunity, December 2014.

[3] D. V. Dimitrov. (2016, Jul). "Medical Internet of Things and Big Data in Healthcare." Health Inform Res. [Online]. 22(3), pp. 156-163. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4981575/ [Jul. 31, 2016].

[4] L. Zhang. "Applications of the Internet of Things in the Medical Industry." Internet: https://dzone.com/articles/applications-of-the internet-of-things-in-the-medi-1, Jun. 24, 2018.

[5] G. Alex, B. Varghese, J. G Jose, A. M. Abraham. (2016), "A Modern Health Care System Using IoT and Android". International Journal on Computer Science and Engineering (IJCSE), vol.8. Issue.4, [Online]. Available URL: http://www.enggjournals.com/ijcse/doc/IJCSE16-08- 04-031.pdf. [Accessed: 11-Nov-2018]

[6] Z. Pang, "Technologies and architectures of the Internet-of-Things (IoT) for health and well-being," Ph.D. dissertation, Dept. Electron. Syst., School Inf. Commun. Technol., Royal Inst. Technology (KTH), Stockholm, Sweden, 2013.

[7] L. Li and W. Benton, "Hospital technology and nurse staffing management decisions," J. Oper. Manag., vol. 24, no. 5, pp. 676–691, 2006.

[8] L. Li and C. Markowski, "An analysis of hospital capacity management patterns using Miles and Snow topology," Int. J. Manag. Enterp. Dev., vol. 3, no. 4, pp. 312–338, 2006.

[9] E. Becker, V. Metsis, R. Arora, J. Vinjumur, Y. Xu, F. Makedon, "SmartDrawer: RFID-Based Smart Medicine Drawer for Assistive Environments," Proceedings of the 2nd International Conference on Pervasive Technologies Related to Assistive Environments, PETRA, 2009, DOI: 10.1145/1579114.1579163

[10] S. Bhati, H. Soni, V. Zala, P. Vyas, Y. Sharma. (2017, April) "Smart Medicine Reminder Box," International Journal of Science Technology & Engineering. [Online]. 3 (10). Available: http://www.ijste.org/articles/IJSTEV3I10093.pdf

[11] N. U. Nyapathi, B. Pendlimarri, Karishma, Kavya," (2016, May) "Smart Medicine Box using ARM 7 Micro controller", International Research Journal of Engineering and Technology (IRJET). [Online]. 3 (5). Available: https://www.irjet.net/archives/V3/i5/IRJET V3I5569.pdf.

[12] V. Shah, J. Shah, N. Singhal, H. Shah & P. Uapdhyay. (2016) "Smart Medicine Box," Imperial Journal of Interdisciplinary Research (IJIR). [Online]. 2 (5). Available: https://www.irjet.net/archives/V3/i5/IRJET-V3I5569.pdf.

[13] PritiBedmuttha, Nisha Jain, YaminiThigale, SatyajitGargori,, Prof. T.R. Patil (April, 2014). "A HEALTH-IOT PLATFORM BASED ON THE BIOSENSOR AND INTELLIGENT MEDICINE BOX". International Journal of Computer Science and Mobile Computing, Vol.6 Issue.4, pg. 433-43, [Online]. Available: https://www.ijcsmc.com/docs/papers/April2017/V6I4201 794.pdf [Accessed: 11-Nov-2018].

[14] Maxim integrated Products. "DS3231 Extremely Accurate I2C Integrated RTC Datasheet" (2010, June) [online]. Available: https://

datasheet.maximintegrated.com/en/ds/S3231.pdf. [Accessed: 11- Nov-2018].

[15] Circuit Basic. “I2C Communication Protocol”. [Online]. Available: http://www.circuitbasics.com/basics-of-the-i2c-communication protocol/. [Accessed: 11-Nov-2018].

[16] Www.einstronic.com. (2017, July 2). “Node MCU ESP8266” [Online]. Available URL: https://einstronic.com/wp content/uploads/2017/06/NodeMCU-ESP8266-ESP-12E Catalogue.pdf. [Accessed: 11-Nov-2018].

[17] NodeMUC8266 Wi-Fi module: “Node MUC 8266”. [Online]. Available URL: http://www.handsontec.com/pdf_learn/esp8266- V10.pdf [Accessed: 11-Nov-2018].

[18] Techopedia “Serial Communication of devices” [Online]. Available URL:https://www.techopedia.com/definition/22010/serial communication. [Accessed: 11-Nov-2018].

[19] ManTech Electronics. (2017). “LCD 2004 Datasheet” [Online]. Available URL: http://www.mantech.co.za/datasheets/products/lcd2004-i2c.pdf. [Accessed: 27-Nov-2018].

[20] Spark fun, Dallas Semiconductor “DS18B20 Digital Temperature sensor” [Online]. Available: https://cdn.sparkfun.com/datasheets/Sensors/Temp/DS18B20.pdf. [Accessed: 27-Nov-2018]

[21] Sashavalli Maniyar, Microchip Technology, “1 wire communication protocol” [Online]. Available: http://ww1.microchip.com/downloads/en/appnotes/01199a.pdf. [Accessed: 27-Nov-2018]

[22] If This Then That (IFTTT) home page. “IFTTT a free web based service” [Online]. Available: https://ifttt.com/create. [Accessed: 27- Nov-2018] 6 Authorized licensed use limited to: Carleton University. Downloaded on August 06,2020 at 14:37:25 UTC from IEEE Xplore. Restrictions apply.