International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 12 | Dec-2017 www.irjet.net p-ISSN: 2395-0072

Secure Cloud Based Centralized Health Improvement through homomorphism Encryption

Shraddha T. Shelar[1], Deepali D. Rane[2], Suraj Rasal[3] , Shubham Davate[4]

[1,2] *Assistant Professor, D. Y. Patil College of Engineering, Pune, Maharashtra, India*
[3] *Assistant Professor, Bharati Vidyapeeth University College of Engineering Pune, India, India*
[4] *Student, D. Y. Patil College of Engineering, Pune, Maharashtra, India*

Abstract – *Every individual on this earth lives with generation lifestyle irrespective of health concern. Nobody gives time for their health seriously, doesn't keeps history record and avoids healthy environment to survive due to fast growing life-style. Even he/she visits hospital for minor health issue, later ignores precautions and treatment cause. But due to ignorance anyone's health can be possibly reflected into major serious health issue which further takes anyone between life and death. Hence, considering these all scenario, it is very essential for everyone so as to take care of their health as first priority of their life. This paper represents very useful medical science application for overcoming such facts. Here we have presented idea of online scheme for sharing, transferring, storing and maintaining database related to person's health. For this, we have used technique of modern cryptography specifically a homomorphism encryption technique and applied for attributes based encrypted data of every patient. Our scheme will also provide the service for patient for finding best doctor for best treatment. This uses third party for storage and authentication scheme for sharing keys between server and patient. Henceforth, our system will surely useful for medical science field for providing best treatment to patients and to give satisfaction for every individual in view of their health.*

Key Words: Attributes, Cryptography, Encryption, Decryption, Homomorphism, Public Key, Secret key

1. INTRODUCTION

Information security is growing high for providing highly secure environment on web to store person's information. Additionally, most of people don't want to do their work as paper based stuffs so as to preserve their previous records. Online storage is the best way to provide such a services for users. But as the number of users increases it is very challenging job for online service providers to give secure storage servicer. If we consider an example of hospital then many times, if say patient A consults one doctor say D for health issue, D will check his previous reports or medical history. But, sometimes patients misplace his data due to long gap in consultancy. If that patient has not carried his data physically with him, then doctor again starts from initial stage of treatment. Hence it will be very important for that doctor so as to know the patient's actual medical history as well as patient will also face the difficulties in proper consultancy of getting medicine or health related checkups. It is obvious that doctor may consults as per their knowledge and experiences but when point comes to check the patient's medical history, doctor may face problems regarding patients allergenic behavior towards medicine or any reaction cause due to improper dose of medicine or type of medicine used. In rare cases, patient may get suffered from improper or wrong consultancy of doctor. This may creates very serious health issue for patients due to which many times patient may suffer between life and death. Henceforth, it is very serious issue taken into consideration for every individual for correct measure of any person's health and providing corrective measures through proper consultancy. It can only be happened by keeping patients previous medical record safely and showing it to current doctor for suitable treatments so as to cure with deceases and get better health.

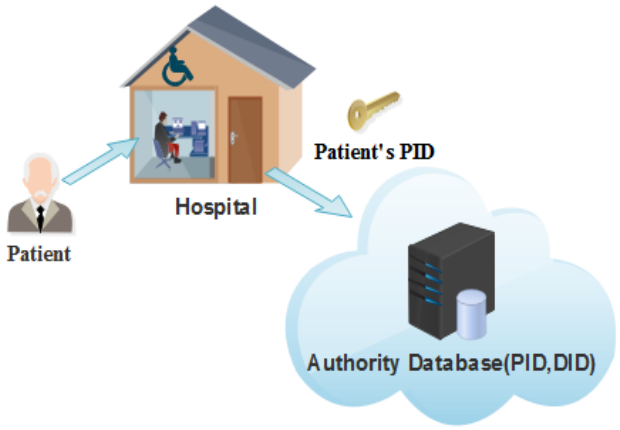

Fig -1: Cloud based secure system Deployment

This paper is specifically focuses on the issue of medical health record storage and its awareness for which there should be standard centralized platform used by all the doctors before starting with suitable Treatments on that patient. It will specially used for the purpose of detecting actual cause of patients and providing corrective measures based on it through his/her medical history. This approach based on two aspects. Fist, it include the central online facility for storing patient's medical history as patients ID PID, doctor's name, medical cause, medicines , reaction cause, improvement plan and remark. On the other side, it also includes doctor's registration number DID, Specialization, feedback rating report. With these two type

of data doctor can make specific decision on patient so as to do a treatment. Additionally, patient will be aware about which doctor is suitable for him depending on that doctors rating. Here, in between this, there should be trustworthy channel provided for maintaining confidentiality in online storage. Hence, this paper represents a best practice of efficiently maintaining

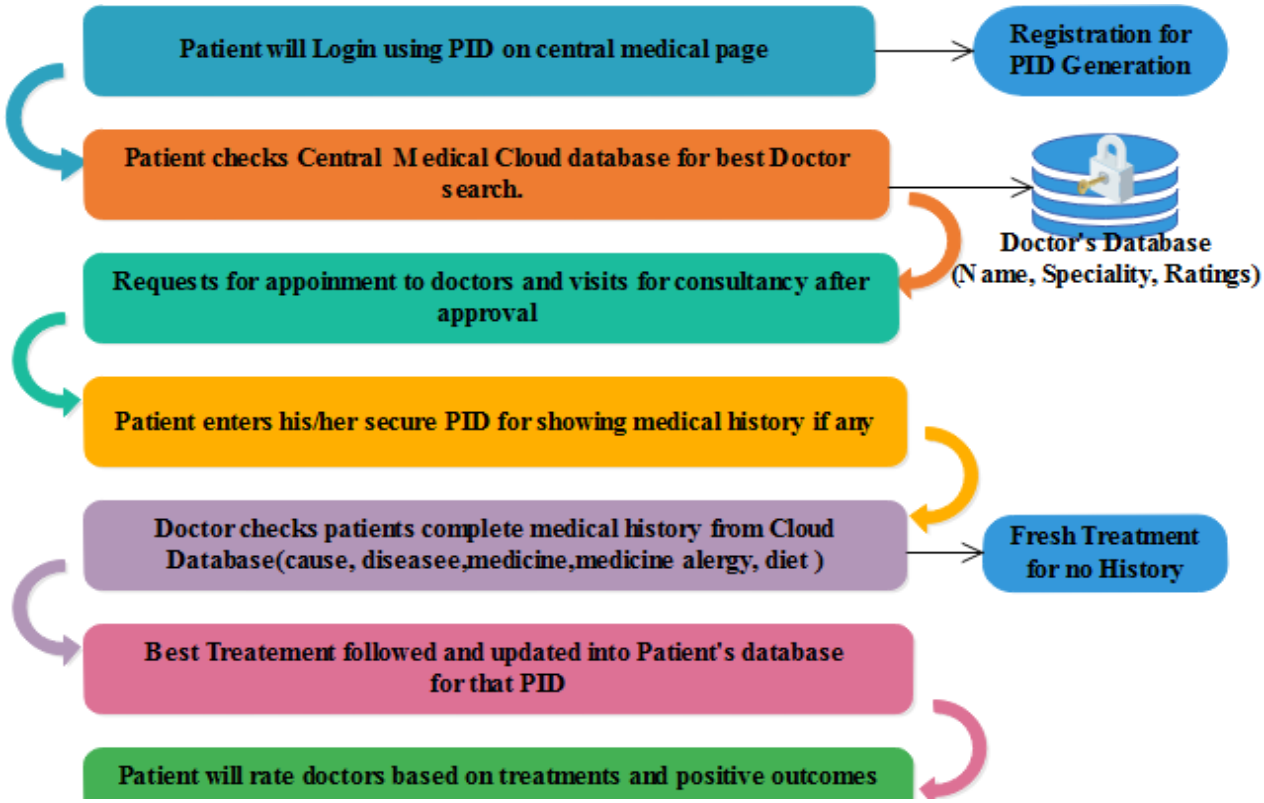

Fig -1: Activity for Centralized Medical database system used in Medical Science

secure and long lasting medical database. This will truly provide patient to get treatment from best doctor as well as it will help doctor to provide specific and best by looking into patient's medical history.

There are many encryption techniques can be applied for providing confidentiality in cloud. But traditional schemes are not long lasting and good enough to provide trustworthy servers when data is big enough in cloud. Hence, modern cryptography has been recently joined the field of cryptography where complete protection package has been provided even for huge amount of data on web.

In this paper, we have discussed homomorphism encryption techniques in public key cryptography for privacy preserving secure medical database. We have presented best approach towards possible outcomes of this skim and shown future usefulness of this database towards time leading process in medical science research field.

2. HOMOMORPHISM FOR CLOUD DATA

Cloud is a very large and distributed concept of today's online storage scheme, where any type of data in any quantity has been stored tremendously. This data may be used as personally or for professional use which is important to keep in safe way. But, any service provider of cloud may not give a commit words about providing confidentiality and integrity of data stored on cloud. There are many cryptographic techniques has been applied. Homomorphism is the best technique to use for internet services where it plays very important role in cloud computing security [3]. When it is used, original data has been not seen while applying encryption technique. This is the major role played by homomorphism that your original data has been not come into picture at all for encrypting it. When patient registers and stores data on cloud it is in encrypted form for safe storage. When other parties wish to explore the information of that patient, it is operated in encrypted format.

When patient himself approaches to do so then only data will be truly shown in its original form. In this work. When patient register to network for storage of data, keys are created for encryption of information and stored on online cloud into medical database. Basically, homomorphism is the technique for already encrypted data which leads to the double encryption for information. So here there is no right to third party for accessing bit of original information not even knows the type of data. The strangeness of this

technique will truly useful in providing the fruitful services in medical science field . It also maintains the records of best doctors to approach for getting benefit of best treatment. Hence this paper is providing possible outcomes for using this online database technology in medical science field.

3. PROPOSED APPROACH

Life is the most important priority of every individual and which should be considered first. But due to very busy schedule no one is ware about if there is not any major concern about health, if there is no any serious issues happened regarding health. If it is satisfied through small and short tablets and oral treatments then not single identity on earth considers it for granted is very big thing happened to his/her body. Henceforth considering to all the aspects of fast going life-style, we have presented a fresh approach of handling the health of every individuals on earth through secure medical technology which will positively work in current aspects of lifestyle.

Figure 2 shown above will explain the architectural view of how this application will work. This paper is only presenting the idea for medical science and for involving it into all over world as government based activity. Because, it will effect on every person's health. When any individual wants first time medical health checkup he/she has to register online on the medical official website. This will generate one PID number for everyone those who will register. So, when he or she wants to consult himself/herself. It is will be mandatory for them to enter PID for knowing medical history if any so as to provide specific and best treatment by doctor. As like patient , every doctor who is doing practice in medical science field should also register himself/herself for getting their DID(Doctor's Identity) which will be used every time when every patient visits at their place. This will help that doctor too for their future ratings by patients, for their service improvement too. When PID and DID has been entered then only patient's data will be shown through server's databases. Hence , for patient also it is necessary to take consultancy from specific doctor. Thus, following steps will simply explain the basic model about how this approach can be implemented for very essential use in medical science.

3.1 Registration Process

This is the initial procedure has to be done by patient/client as well as doctor. When one patient want to consult by doctor he/she will register himself/herself through online scheme. Here it is necessary to check the authorized user by uploading his/her identity documents so as to avoid the threats in system. After this, patient will receive PID number (PIDSk) which is technically secret key generated by server side. Doctor also has to gain registered ID(DIDSk) before starting with his/her career in medical science field. In this step, both doctor's and patient's database has been maintained separately and stored in encrypted format using public keys generated (PIDPk). So, on server data stored is t in original format and encrypted on server side. It gives the direct access to third party which is heedfully has to be kept in encrypted format. As data is regarding patient's as well as doctor's credential there should not be any sort of access and rights provided to third party server. Hence, we have came up with possible solution by using additive and multiplicative feature of homomorphism encryption. This has been applied on data as well as key of users. Previously it has been only applied to information on cloud for storing the data but here keys are also target point for any kind of attacks like DoS or Man-in-Middle attacks [1] which needs to overcome also. Hence, Here both will register and will store their identity on server with keys but in encrypted format. This process basically uses attributes sets for encryption [2]

3.2 Homo-mechanism for cloud data

This uses EIGmal cryptosystem and Gentry's cryptosystem [5][6] to construct the properties on already encrypted data. With this, it is possible to perform the complex calculation of addition and multiplication on cipher text. When data encrypted on already encrypted information then there is only need of approval for its decryption by the owner of that data. Here when homomorphism has been applied on encrypted data old data get lost automatically which is stored on third party.

3.3 Access control on personal database

When any patient who is registered for online medical database initially takes appointment for treatment online. First best doctors will be displayed as per the ratings given by previous patients to them. Patient will select as particular doctor as per his/her specialization. For example. For neural issues patient will see the list of all neurologists in list as per the selected information. He or she will take appointment and will visit that place for consultancy.

When patient will enter his/her PIDSk on platform of database followed by that doctor's DIDSk. Initially data will be in homo-encrypted format on server. When this has been entered by both side then only all the information of patient has been displayed to doctor for further consultancy. It is essential for every individual to keep information most secure on cloud. Her Information of patient and doctor's credentials are stored as well as patient's complete information of his/her medical history, previous cause, allergy medicines, pervious doctor's information and consultancy remarks are mentioned in database. The motto behind this approach is clear towards strongly securing information as well as providing trustworthy access control for using this platform. Also if this service has been used as it is giving solution of double encryption through best feature of modern cryptography

4. CONCLUSION

This paper presents possible outcomes specifically for medical science field for maintaining best platform for

patient doctor relationship. It uses most secure technique for storing and accessing cloud based data for which patient s well as doctor's approval needed. It has avoided giving rights to third party server for looking into data and applied technique on cipher text for both keys and data. It will also save every individual's time for finding best medical service for their health by providing highly rated medical specialist list in very short time. Hence, this all aspects will truly useful for improvement and enhancement of every body's health if best treatment found which is possible through our centralized secure communication system.

REFERENCES

[1] M. Abdalla, M. Bellare, P. Rogaway, "DHAES: an encryption scheme based on the Diffie–Hellman problem", IEEE P1363a, 1998.

[2] Shraddha Rasal, "Enhancing Flexibility for ABE through the Use of Cipher Policy Scheme with Multiple Mediators", Springer's Advances (AISC). November 2014.

[3] Craig Gentry "a fully homomorphic encryption scheme", September 2009.

[4] Yi. X. Paulet, R. Bertino .E, "Homomorphic Encryption and Application," Springer, Page no 27-46, 2014.

[5] ElGamal, "A Public Key Cryptosystem and a Signature Scheme based on Discrete Algorithms", IEEE transaction theory, Vol no 4, July 1985.

[6] Van Dijk, M., Gentry, C., Halevi, S., & Vaikuntanathan, V. "Fully homomorphic encryption over the integers" EUROCRYPT2010pp.24–43.Berlin:Springer. doi:10.1007/978-3-642-13190-5_2,2010