A Classical Method for Health Monitoring on IoT: From Architecture, Security & Application

Adarsh T K, K P Vijayakumar

Abstract*: *The development of smart health care monitoring systems, and services is driven by the development of the Internet of Things (IoT). IoT devices produce major role in todays healthcare monitoring systems large number of systems are in this field developing to track health data. The data generated by these devices has to face numerous security related requirements in order to be useful in real life. Among these one of the requirements is provide a detail approach to meet complete intelligent system to monitor health records, The theme proposed here is collect data from multiple sensor use and filter useful information about present state for identifying and integrating the health status of a person. Apart from this how to share health data in secure platform and authenticated architecture node in IoT. In proposed work describes the usage of IoT in health care data in a classical manner which in bounded in an architecture and system devices.

Key words: IoT (Internet of Things), AU, Medical Electronic Health Record.

I. INTRODUCTION

Last few years have seen a rising demand for wearable sensors and today enormous gadgets are available in the industrially accessible [1] for individual human health services, Due to the evaluation of Internet of Things (IoT) a vital role in this paradigm shift and become systems go “smart”. Thus a new ecosystem of smart phone, smart environment, smart health care, etc., represents how IoT utilizes new in the new era of intelligent methods in connecting services. The main objective is data from these all inter-connected systems can be accessed according to users availability and needs, using any network [2].

Utilizing the collected information, and data analytics helped by decision making that perception information for different people, Such innovation could create drastic affect worldwide medicinal services and definitely reduce human services costs and improve speed and analyze. In rural area most of the peoples does not gets appropriate treatment to health monitoring and clinics. Hence it is necessary to develop an effective health monitoring system that helpful for all in urban as well as rural area. However, wearable sensors have, lead role in this point on the current clinical framework.

The device should play a vital role in data confidentiality, integrity, [3]availability and authentication depending on EHR, Current scenario is introduce malicious nodes , since the record shares between patent, doctor and care taker ABE(attribute based encryption) provides a method to access control in medical data system. The user are assigned to secret key and patients EHR are encrypted.

1.1 Our Motivation

To over come above challenges a classical model to maintain privacy from architecture through application in health monitoring IoT id designed and main contribution is discussed below

- Authenticate device registration

The identification of patients and medical nodes are important in order to meet the above constrain every device should register by sharing a key to authenticate in IoT network. This will achieved by generating a key by patient and share to medical nodes and this will authenticate weather this message is send by patient IoT network.

- Authenticate key generation and exchange

After the key is extracted by the medical node the message generated will encrypted and send back to patient to make sure that authenticity of source, This authentication done by key generated by patient using AU(Authentication Unit) setup algorithm

- MEHR encryption and decryption

Medical Electronic Health Record are encrypted the procedure for doing so is from the key generated by AU, This system is also provide dual verification for improve efficiency, the patient can also recover the encrypted data.

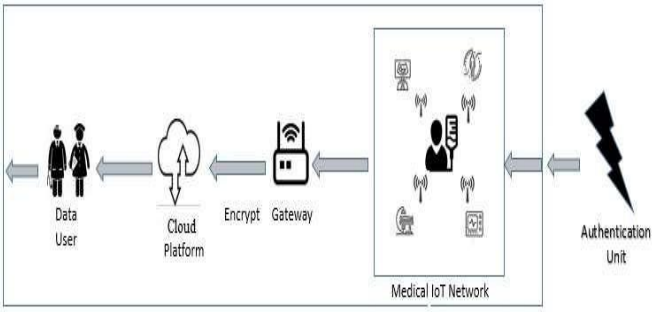


Fig. 1. System Architecture Model

Simplex access update

The MEHR is stored in cloud after encryption in order to preserve security an simple access update policy in introduced when a user wants to update access. The server will get updated with out relieving the health data, The knowledge of data remain secure and only the access policy will get update depending on users request.

Revised Manuscript Received on September 22, 2019.

Adarsh T K, Department of CSE SRMIST, Chennai, India email: adarshtk@gmail.com.

Dr. K P Vijayakumar, Department of CSE SRMIST, Chennai, India email:vijayakumar.kp@ktr.srmuniv.ac.in

1.2 Related work

1.2.1IoT and health monitoring system

In the early survey IoT(Internet of Things) network explains the major development in medical health monitoring is widely adopted, The development of IoT in recent medical field gives much challenges in relevant field. The authors summarized[4-5] the evolution of IoT and related medical health monitoring, The data tracking as well as security in different stages is maintain at the same time few researcher focus on data provenance to meet the requirement, few health monitoring hardware are Pulse Oximeter, Temperature sensor, RFID, PIR- Passive infrared Detects heat of a body. A feasible scheme required to develop for proper health monitoring framework.

1.2.2Key generation and encryption

There are enormous technology for generating key for encryption and algorithms for encryption The searchable proxy re-encryption is investigated in [9] to resist post quantum attack. Cao et al.[10] construct a rank scheme supporting multiple keywords and Cash et al[11] discuss dynamic searchable encryption system. Yang et al explains the flexible conjunctive keyword search and some other works is proposed get keyword search. The concept of encryption by Goyalet al.[12] is ABE attribute based encryption at the same time policy of updating in [13] to develop different scheme.

1.3 Road map

The rest of the paper is planned as follows, In section 2 Architecture and Security model are introduced. Section 3 described proposed system for security and its application in health care monitoring IoT networks. Section 4 explains discussion, finally in last section gives conclusion of paper.

II. ARCHITECTURE AND SECURITY MODEL

2.1 System Architecture and Security Model

The system architecture for the proposed system in depicted in Fig.1. The different actors involved is

- Authentication Unit(AU): It is completely trusted device in the system that to generate global secret key and also to generate secret key for patients and users, The entire system is works based on the global key generated that become backbone to the ecosystem.
- Medical IoT network: This consist of patient and medical nodes in which the medical reports is monitor by this network, Patient node generate secret key pair for medical node it also deals with security. The Medical Electronic Health Record(MEHR)is encrypted by Patient using global key generated by AU and Medical node duty is to collect medical data and encrypt using global key and sends back to patient.
- Cloud Platform: Here the storing of encrypted MEHR it's a secure and privacy hub, Another major feature is when a keyword received from patient its shares and update the access policy so that at any time of need to update the update access policy is relevant.
- Users: Normally Doctor, Nurse and caretakers are under this category when a secret key receives it encrypt MEHR, They can view the medical record in a secure manner and uses

update access policy for further updating in access to the health record.

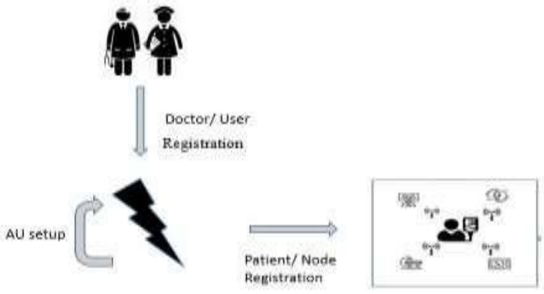


Fig. 2. AU setup and registration

The second and important level is to provide security and privacy preserving model in order to maintain this executed in three phases, setup phase, key generation and encryption phase, update and access phase.

Setup Phase: An global key generation algorithms is executed in AU and parameter is generated. That is shares to Y and GSK kept secret from Y, In key generation and encryption phase: A list of query associated is executed by Y, like patient mark, nodes and users secret key generation an algorithm runs on basic of GSK, it is required that secret key of attributes satisfies the access policy. In third phase except attribute of secret key the update policy will runs and allowed to be updated.

TABLE I: NOTATION

Notation	Description
AU	Authentication Unit
MEHR	Medical Electronic Health Record
GSK	Global Secret Key
PA	Patient
MN	Medical Node
m	Message in IoT
M	Health record in IoT
K	Security parameter
AUQ	Access update query
SEnc/SDec	Security key encryption and decryption

III. PROPOSED SYSTEM

In the coming section a classical approach for health monitoring in IoT health care systems with complete architecture and security provided, the used notation are defined in table1. This frame work will consist of different phases explained in fig 2-4 and followed by security preserving system.

As shown in fig 2 Authentication Unit(AU) runs algorithm to generate GSK at the same time it generate patient secret key pair after the patient registration .In the figure3 the MN execute message encryption and aggregate to form MEHR and that to be stored in cloud platform that should be accessed by data user and finally in figure4 the process of updating is explained. In update policy an Policy update query (PUQ) submitted in cloud with patient keyword it will be updated. The following security requirements had meet,

3.1 Patient and Medical node traceability

When a patient and Node resisted an identity is generated using GSK and if we found any misbehavior it can trace easily

3.2 Authentication and Confidentiality of IoT Message:

With the help of IoT message encryption and decryption algorithm the confidentiality of message is guarantee by doing the verification the authentication is also maintain. Thus in proposed system the following approach is executed

- Data collection and Preprocessing
- Encryption and Security
- Authentication Unit (AU)
- Storage of data in cloud

The above mention points are detail in during the simulation stage. Using PCB (pairing based cryptography) library is used for simulation.

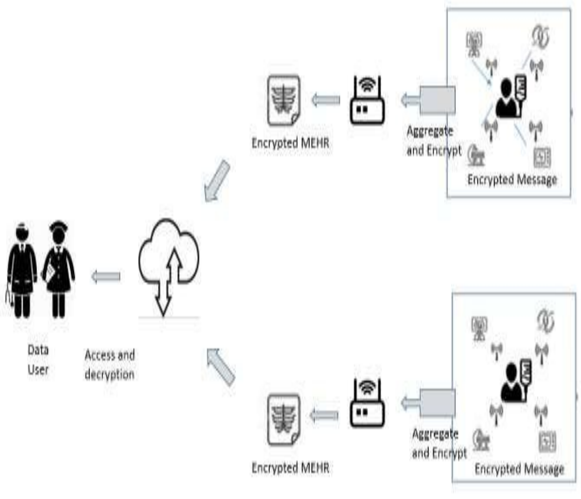


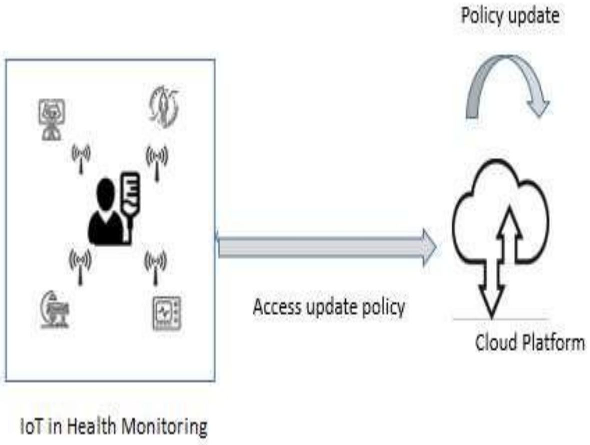
Fig. 3. MEHR encryption and security

3.3Security against access update

The process of key distribution is major issue faced in authenticated health care IoT, to over come this a timestamp is introduced at patient side algorithm that indicate key generation period. And during the time of encryption Ts is selected by node to indicate in encryption.

IV. DISCUSSION

The proposed framework and other existing systems are evaluating using simulations and uses PCB library. And following points are noted. The transmission efficiency of various parameters in different schemes with our scheme are found much better this shows the transmission costs is also very low, another point is computational efficiency and the computational cost of MEHR file encryption is expected to found in large decrease since the number of keyword is used in proposed is comparatively very feasible.



f Fig. 4. MEHR encryption and security

During the correctness the algorithm proposed are analyzed based on few extraction algorithm with proof of giving sample data sets, few theorems are also evaluated in security proof consideration this case the challenges are also list outs in each phase and corrective measures are taken in further order. In the performance analysis we came to cooperate with existing simulation in terms of costs and keyword used. Few communication as well as computation overheads are listed and found our system is more feasible in model and security wise.

V. RESULT AND CONCLUSION

In the proposed work a classical approach for health monitoring is developed from the architecture level through security and application frame work, in order to maintain security AU setup develop GSK that needful for encryption and decryption for IoT message and finally stores in cloud platform not only this an update policy is also develop when a user request for an update condition satisfies. Patients MEHR are encrypted that provide much security to data services also. The comparison of different policy also gives a clear idea on how much this system is ahead in efficiency and computational level that application level in medical health care monitoring.

REFERENCES

1) A.M. Ghosh, D. Halder and SK.A. Hossain, “Remote Health Monitoring System through IoT” 5th (ICIEV),2016.
2) Min Chen, Yujun Ma, Jeungeun Song, Chin-Feng Lai, Bin Hu, “Smart Clothing: Connecting Human withClouds and Big Data for Sustainable Health Monitoring”, 2016
3) D. Liao, G. Sun, H. Li, H. Yu, V. Chang, The framework and algorithm for preserving user trajectory while using location-based services in IoT-cloud systems, Cluster Computing 20 (3) (2017) 2283–2297.
4) HN Saha, A Mandal, S Abhirup, “Recent trends in the Internet of Things”, 2017
5) B. Farahani, F. Firouzi, V. Chang, M. Badaroglu, N. Constant, K. Mankodiya, Towards fog-driven IoT ehealth:
6) promises and challenges of IoT in medicine and healthcare, Future Gener. Comput. Syst. 78 (2018) 659–676.
7) I. Azimi, A.M. Rahmani, P. Liljeberg, H. Tenhunen, Internet of things for remote elderly monitoring: a study from user-centered perspective, J. Ambient Intell. Human. Comput. 8 (2) (2017) 273289

8) J. Pagn, M. Zapater, J.L. Ayala, Power transmission and workload balancing policies in ehealth mobile cloud computing scenarios, Future Gener. Comput. Syst. 78 (2018) 587–601

9) T. Adame, A. Bel, A. Carreras, J. Meli-Segu, M. Oliver, R. Pousa, CUIDATS: An RFID–WSN hybrid monitoring system for smart healthcare environments, Future Gener. Comput. Syst. 78 (2018) 602–615.

10) Y. Yang, X. Zheng, V. Chang, et al., Semantic keyword searchable proxy reencryption for postquantum secure cloud storage, Concurr. Comput.: Pract.Exper. 29 (19) (2017).

11) N. Cao, C. Wang, M. Li, et al., Privacy-preserving multi-keyword ranked search over encrypted cloud data, IEEE Trans. Parallel Distrib. Syst. 25 (1) (2014) 222– 233.

12) V. Goyal, O. Pandey, A. Sahai, et al., Attribute-based encryption for fine-grained access control of encrypted data, in: Proceedings of the 13th ACM Conference on Computer and Communications Security, ACM, 2006, pp.89–98

13) K. Yang, X. Jia, K. Ren, Secure and verifiable policy update outsourcing for big data access control in the cloud, IEEE Trans. Parallel Distrib. Syst. 26 (12) (2015) 3461–3470.

14) Y. Miao, J. Ma, X. Liu, et al., Attribute-based keyword search over hierarchical data in cloud computing, IEEE Trans. Serv. Comput. (2017)

15) R. Snader, R. Kravets, A.F. Harris III, CryptoCoP: Lightweight, energy-efficient encryption and privacy for wearable devices, in: Proceedings of the 2016 Workshop on Wearable Systems and Applications (WearSys'16), ACM, New York, NY, USA, 2016, pp. 7–12. http://dx.doi.org/10.1145/2935643.2935647.