IoT based Smart Hospital for Secure Healthcare System

Sejal Patel
Computer Science & Engineering
Parul Institute of Engineering and Technology,
Vadodara, Gujarat, India.
E-mail:*sejupatel02@gmail.com*

Narendra Singh
Computer Science & Engineering
Parul Institute of Engineering and Technology,
Vadodara, Gujarat, India.
E-Mail: *narendra.singh@paruluniversity.ac.in*

Sharnil Pandya
Information Technology
Parul Institute of Engineering and Technology,
Vadodara, Gujarat, India.
E-Mail: *sharnilpandya@paruluniversity.ac.in*

***Abstract*—**Now a day, with the rapid use of internet and implementation as well as development of medical sensor for healthcare applications, Internet of Things (IoT) has gained raising popularity. IoT is the paradigm of connectivity, sensor connected with the embedded system. All sensor and device connected to each other so transmission and communication between those sensors become easily. In healthcare system the medical data are sensitive in nature so without considering security and privacy is worthless. Cloud computing is the most important paradigm in IT-health. All the medical data of the patient as well as the doctor and patient personal information store in local mode as well as cloud, so whenever it needed the data will be easily available.Patient medical data is stored in system as well as cloud, so malicious attack and unwanted access may cause a harmful to patient health. Security is most important and crucial part of healthcare. The access control policy is based on right to access of medical data and privilege to authorized entity which is directly and indirectly connected with the patient health.

Keywords*-Internet of Things (IoT), security, privacy, access control,cloud computing.*

*****

I. INTRODUCTION

Internet of Things (IoT) is an ideal extensive technology to effective the internet and communication technologies. In the General way Internet of Things is an approach to connect living and nonliving things with the help of Internet. In traditionally way everything in the world is conceive as an object, but in the IoT paradigm everything in the world is considered as a smart object, and allows them to communicate each other through the internet by physically or virtually. IoT get approval to people and things to be connected and communicate Anytime, Anyplace, with anything and anyone [19].

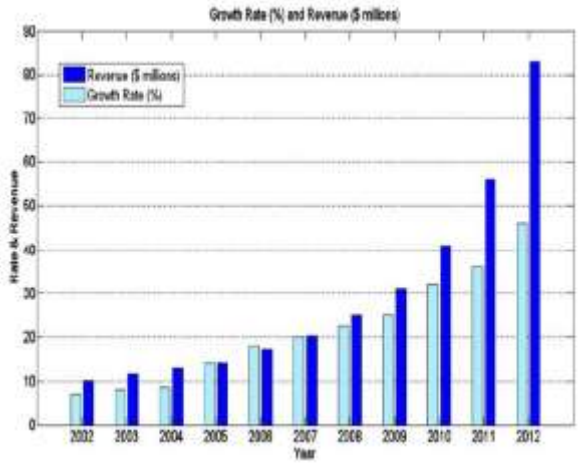

Figure 1: The Growth Rate and Revenue for healthcare

Very huge medical information which is sensitive in nature is being collected, transmitted, stored, and shared among different medical organizations.Enormous transaction of such electronic and even exchange and transmit personal and medical information is offered through the Internet [7]. Therefore, it is clear, specific measures are necessary to ensure that patient medical data can access some authorized person not everyone. For the purpose, privacy of data and security privacy, it will be necessary to authorized can access the data and according them to perform the task, and the data could be obtained.

The problem of security is rising nowadays. However, especially the privacy of communication through Internet may be at risk of attacking in a number of ways. On-line collecting, transmitting, and processing of personal data make up a severe threat to privacy. Once the utilization of Internet-based services is concerned on-line, the lack of privacy in network communication is the main conversation in the public. This problem is far more significant in modern medical environment, as healthcare networks are implemented and developed. According to common standards, the network linked with general practitioners, hospitals, and social centers at a national or international scale. While suffering the risk of leaking the privacy data, such networks can reduce the costs and improve the effectiveness of the healthcare system.

Generally speaking, intruders include hacker, spies, terrorists, co-intruder, and profession. They use operator

commands, macro, and Java Script to break through a computer network with the purpose to retaliate, steal confidential information, and fulfill themselves' senses of accomplishment. For a further conclusion, their success depends on some current problems in the whole computer networks, such as errors in network framework design, management negligence, illegal downloading.

II. RELATED WORK AND MOTIVATION

The advancement of healthcare system have made patient monitoring more feasible. Recently, several wireless healthcare researches and projects have been implied, which can aim to provide continuous patient monitoring, in-ambulatory, in-clinic, and open environment Monitoring. In this area, an outline of these advances, alongside their possibility, is given.

CodeBlue [6] is in-vogue healthcare research project based on developed at Harvard Sensor Network Lab. In this project, many cheap bio-sensors are placed on patient's body. These sensors sense the patient body and transmit it wirelessly to the end-user device (PDAs, laptops, and personal computer) for further analysis. The basic idea of the CodeBlue is straightforward, a doctor or medical professional issues a query for patient health data using their personal digital assistant (PDA), which is based on a published and subscribed architecture. Besides, CodeBlue's authors acknowledge the need of security in medical applications, but until now security is still pending or they intentionally left the security aspects for future work.

Subsequently, another healthcare research project named was Alarm-net, which is designed at the university of Virginia [7]. The project is specifically designed for patient health monitoring in the assisted-living and home environment. Alarm-net consist of body sensor networks and environmental sensor networks. Besides, the authors have pointed out some confidentiality infringement scenarios on Alarm-net, but some security parameter still pending or we can say that as an address to as a future work.

Meanwhile, another healthcare system was designed by Ng et al, named UbiMon [10] was proposed in the department of computing, Imperial College, London. Theaim of this project was to address the issues related to usage of wearable and implantable sensors for distributed mobile monitoring. Although Ng et al. proposed and demonstrated the ubiquitous healthcare monitoring architecture, it is widely accepted that without considering the security for wireless healthcare monitoring, which is a paramount requirement of healthcare applications, according to government laws.[11]

Chakravorty designed a mobile healthcare project called MobiCare [12]. MobiCare provides a wide-area mobile patient monitoring system that facilitates continuous and timely monitoring of the patients physiological status. Although, Chakravorty acknowledged the security issues in MobiCare, but only addressing security issues are not sufficient for real-time healthcare applications. Thus, security and privacy is still not implemented in MobiCare healthcare monitoring or may have been left out for future work.

As we have seen, all the above ongoing healthcare monitoring projects enable automatic patient monitoring and provide potential quality of the healthcare without disturbing patient comfort. All the projects focus on the reliability, cost effectiveness and power consumption of their prototypes, but although most of the healthcare projects mentioned above addresses the requirement for security and privacy for sensitive data, only a few embed any security. Besides, none of the above projects addressed all the security requirements and their implication, which is greatly imperative for critical applications.

III. SECURITY REQUIRMENTS IN IOT BASED HELATHCARE SYSTEM

Security is one of the most imperative aspects of any system. People have different perspective regarding security and hence it defined in many ways. In general, security is a concept similar to safety of the system as a whole.

A. Authentication

It is one of the most important requirements in any IoT based healthcare system, which can efficiently deal with the impersonating attacks. In healthcare system, all the sensor nodes send their data to a coordinator. Then the coordinator sends periodic updates of the patient to a server. In this context, it is highly imperative to ensure both the identity of the coordinator and the server. Authentication helps to confirm their identity to each other.

B. Confidentiality

Confidentiality is emergent requirement in healthcare system. As health-care records contain sensitive information, the storage systems must ensure their confidentiality. Moreover, only authorized personnel should have access to confidential medical records. Consequently, to ensure confidentiality, storage systems must deploy strong encryption in both the actual storage and the data pathways leading to and out. Moreover, in the case of storage media re-use or disposal, the confidentiality of records previously stored in such media should be ensured.

C. Integrity

The storage system must ensure the integrity of medical records. In particular, it must ensure the integrity of medical records even in the case of malicious insiders. The security mechanisms must identify any tampering of information.

D. Availability

Availability is most important requirement in healthcare system. The health-care records must be accessible in a timely

 ISSN: 2321-8169
404 – 408

manner. Medical records are frequently expanded, and patients may also ask for correction of records. Medical data is always available from its storage when it's needed.

E. Access Control

Access control is of particular importance when the database storing the composite EHR is using a database-as-a-service (DAS) paradigm, where an organization's database is stored at an external third-party service provider. The access control policy is typically based on the privilege and right of each practitioner authorized by patient or a trusted third party. We argue that access control policies should be consistent with the structure of the stored EHR record and the usage of the encryption scheme.

F. Data Privacy

Data privacy is considered to be most important issue in healthcare system. It is required to protect the data from disclosure. It should not leak patient's vital information to external or neighboring networks. In IoT-based healthcare system, the sensor nodes collect and forwards sensitive data to a coordinator. An adversary can eavesdrop on the communication, and can overhear critical information. This eavesdropping may cause severe damage to the patient since the adversary can use the acquired data for many illegal purposes.

IV. PROPOSED WORK

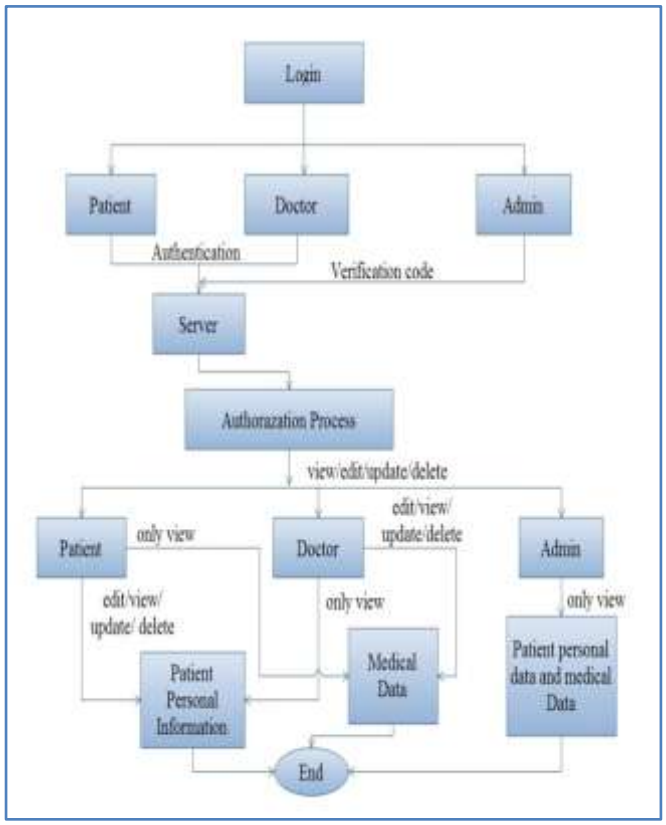

Figure 2: Proposed Design scenario1

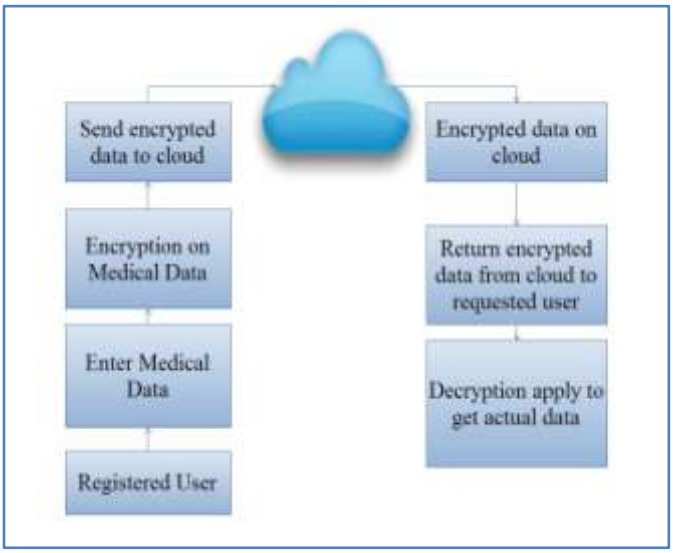

Figure 3: Proposed Design scenario2

The main objective of the proposed work is to resolve several security issues existing in healthcare system and also to guarantee reasonable computational overhead.

TABLE I
NOTATIONS

μ : Unique ID
p : patient
d : doctor
ID_d : patient unique id
ID_p : doctor unique id
n_g : random number generate by server
k_p : secret key for patient
k_d : secret key for doctor
PU_s : server public key
PR_p : private key for patient
PR_d : private key for doctor
E : Encryption
D : Decryption

Scenario 1: The process of the access control and authentication mechanism
Input: Unique ID for patient & doctor
Output: allow to access medical data
Begin

1. Initialization process
2. μ is the unique Id which having p & d has registered user
3. if μ ϵ p, d
   then login and go to step 4
   else
   firstly patient & doctor go to administration and need to add some general information

4. system will check whether p, d has to be authorized or not
   if p, d authorized then go to step 5
   otherwise go to step 1
5. after authorization process system will check whether user is patient , doctor or admin
   if patient – can edit/view/update/delete their personal information but he/she can't able to modify the medical data
   if doctor – can edit/update/view patient medical data accordingly their disease
   if admin – can be edit/update/view/delete all the data
6. End

Scenario 2: The process of the encryption and decryption

1. A new user p and d submit their unique identity μ to the server
2. After receiving the request from p & d server generate random number n_g and compute secret key for p & d.
   secret key k_p = h($_p||n_g$) and = k_d h($_d||n_g$) respectively and transmit to p & d.
3. Encrypt data with server public key PU_s, E(PU_s, k_p) & E(PU_s, k_d)
4. Encrypted data will be store on the cloud
5. In the time of receiving the data, patient and doctor decrypt the data with their private key
   D (PR_p , E(PU_s, k_p)) and D (PR_d , E(PU_s, k_d))
6. End

In order to analyze the proposed scheme especially in security front, proposed scheme has been compare with various schemes in terms of various security requirements in healthcare system. The proposed healthcare system can satisfy all the security requirement of the healthcare system which is clearly shown in Table II.

TABLE II
Performance Benchmarking Based on Security Requirement

Security Requirement	Code blue	Alarm net	Ubi Mon	Mobicare	Ours
Authentication	Yes	Yes	Yes	Yes	Yes
Confidentiality	No	Yes	No	Yes	Yes
Integrity	No	No	No	No	Yes
Availability	No	No	Yes	Yes	Yes
Access Control	No	No	No	No	Yes
Data Privacy	No	No	No	No	Yes

In the last, proposed healthcare system causes less than half computational overhead and execution time as compared to existing system, which is greatly useful for the resource constrained sensor devices. The detail of the comparison between the execution time and computation cost is shown in Figure 3 and Figure 4.

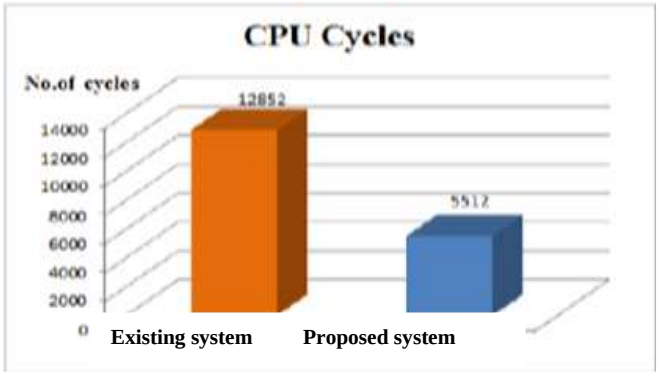

Figure 4: Performance benchmarking based on CPU cycles.

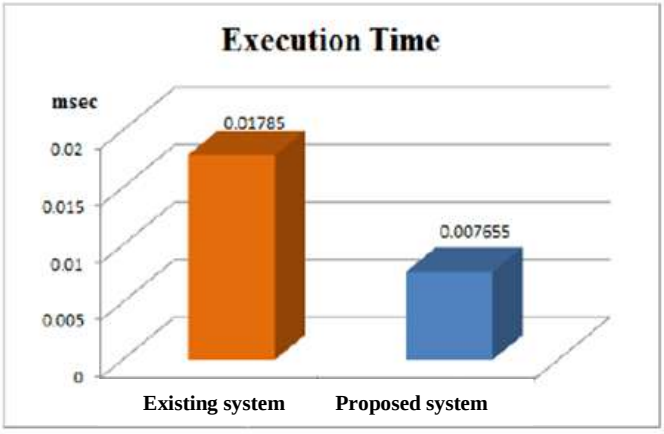

Figure 5: Performance benchmarking based on execution time.

V. CONCLUSION

In this paper, discussed, reviewed and analyzed numerous different security requirements which is used in healthcare system. Most of the popular healthcare based research projects acknowledge the issue of the security, but they fail to embed strong security services that could be preserve patient privacy so the main goal of this work is fulfill all the security requirement in healthcare system.

V. ACKNOWLEDGEMENT

At last but not least, I would like to appreciate all the people who help me directly or indirectly in preparing this research paper.

VI. REFERENCES

[1] T Soren Craig, Sudeer Chinta, Mary Eshaghian-Wilner, Nikila Goli, Aman Gupta and Andrew Prajogi, "Securing Pervasive Communications in Healthcare Systems " *Journal of Advances in Engineering and Technology*, 2016, 3(4): 7-11

[2] Prosanta Gope and Tzonelih Hwang "BSN-Care: A Secure IoT-Based Modern Healthcare System Using Body Sensor Network" *IEEE SENSORS JOURNAL*, VOL. 16, NO. 5, MARCH 1, 2016

[3] Sanaz Rahimi Moosavi, Tuan Nguyen Gia, Amir-Mohammad Rahmani, Ethiopia Nigussie, Seppo Virtanen, Jouni Isoaho, Hannu Tenhunen "SEA: A Secure and Efficient Authentication and Authorization Architecture for IoT-Based Healthcare Using Smart Gateways" *6th International Conference on Ambient Systems, Networks and Technologies* ,Elsevier 2015.

[4] Alavalapati Goutham Reddy, Ashok Kumar Das, Eun-Jun Yoon, and Kee-Young Yoo " A secure Anonymous Authentication Protocol for Mobile Services on Elliptic Curve Cryptography" *IEEE access* 2016

[5] Prosanta Gope, Tzonelih Hwang "A Realistic Lightweight Anonymous Authentication Protocol for Securing Real-time Access in Wireless Sensor Networks" *IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS*, 2016

D. Malan, T. Fulford-Jones, M. Welsh, and S. Moulton, "CodeBlue:An *ad hoc* sensor network infrastructure for emergency medical care,"in Proc. MobiSys Workshop Appl. Mobile Embedded Syst. (WAMES), Boston, MA, USA, Jun. 2004, pp. 1–8.

[6] A. Wood *et al.*, "ALARM-NET: Wireless sensor networks for assistedliving and residential monitoring," Dept. Comput. Sci., Univ. Virginia, Charlottesville, VA, USA, Tech. Rep. CS-2006-01, 2006.

J. W. P. Ng *et al.*, "Ubiquitous monitoring environment for wearableand implantable sensors (UbiMon)," in *Proc. 6th Int. Conf. Ubiquitous Comput. (UbiComp)*, Nottingham, U.K., Sep. 2004.

[7] R. Chakravorty, "A programmable service architecture for mobile medical care," in *Proc. 4th Annu. IEEE Int. Conf. Pervasive Comput.*

Commun. Workshop (PERSOMW), Pisa, Italy, Mar. 2006, pp. 531–536.

[8] Ragib Hasan, Marianne Winslett, and Radu Sion "Requirements of Secure Storage Systems for Healthcare Records" *Springer*, 2014

[9] Mohammed Riyadh Abdmeziem, Djamel Tandjaoui "An end-to-end secure key management protocol for e-health applications"*Computers and Electrical Engineering,ELSEVIER* ,2015

[10] Xingliang Yuan, Student Member, IEEE, Xinyu Wang, Cong Wang, Member, IEEE, Jian Weng, Member, IEEE, and Kui Ren, Fellow, IEEE "Enabling Secure and Fast Indexing for Privacy-assured Healthcare Monitoring via Compressive Sensing" *IEEE Transactions on Multimedia*, IEEE Volume: 18, Issue: 10, August 2016

[11] S. Sicari, A. Rizzardi, L.A. Grieco, A. Coen-Porisini "Security, privacy and trust in Internet of Things: The road ahead" Computer Networks, *ELSEVIER* ,2015

[12] Liping Zhang & Shaohui Zhu "Robust ECC-based Authenticated Key Agreement Scheme with Privacy Protection for Tele-care Medicine Information Systems", *Journal of Medical System* ,Springer 2015

[13] Debiao He and Sherali Zeadally "An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography",*IEEE Internet of Things Journal Volume: 2, Issue: 1*, Feb. 2015

[14] P. Kumar and H.-J. Lee, "Security issues in healthcare applications using wireless medical sensor networks: A survey," *Sensors*, vol. 12 no. 1, pp. 55–91, 2012

[15] P. Gope and T. Hwang, "A realistic lightweight authentication protocol preserving strong anonymity for securing RFID system," Computer security vol. 55, pp. 271–280, Nov. 2015.

[16] P. Gope and T. Hwang, "Lightweight and energy-efficient mutual authentication and key agreement scheme with user anonymity for secure communication in global mobility networks," *IEEE Syst. J.*,doi: 10.1109/JSYST.2015.2416396, 2015

[17] Jin Wang, Zhongqi Zhang, Kaijie Xu, Yue Yin and Ping Guo "A Research on Security and Privacy Issues for Patient related Data in Medical Organization System"International Journal of Security and Its Applications Vol. 7, No. 4, July, 2013