International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 1 | ISSN : 2456-3307

Aadhar Card Based Health Records Monitoring System

V. Saganya[1], Dr. C. Geetha[2]

[1]Department of Computer Science and Engineering RMK Engineering College Kavaraipettai Chennai, Tamilnadu, India
[2]Associate Professor, Department of computer Science and Engineering, RMK Engineering College, Kavaraipettai Chennai, Tamilnadu, India

ABSTRACT

Cloud computing is emerging as a promising paradigm for computing and is drawing the attention from both academia and industry. The cloud-computing model shifts the computing infrastructure to third-party service providers that manage the hardware and software resources with significant cost reductions. It is emerging as a new computing paradigm in the medical sector besides other business domains. Large numbers of health organizations have started shifting the electronic health information to the cloud environment. Introducing the cloud services in the health sector not only facilitates the exchange of electronic medical records among the hospitals and clinics, but also enables the cloud to act as a medical record storage center. Moreover, shifting to the cloud environment relieves the healthcare organizations of the tedious tasks of infrastructure management and also minimizes development and maintenance costs. Storing the medical data in cloud makes the treatment efficient by retrieving patient's medical history from the database before going for the treatment and get to know about the health issues of the patient.

Keywords : *Certificateauthority, Identification Number, Security, Cloud Computing, Denail of Service*

I. INTRODUCTION

A system which handles the medical history of each individual of the country and provides access to all registered hospitals to read or update the data. The hospital which accesses the database must be registered and must have got a license. The license number is used as a unique code to access the database. The details of the patients will be stored and an identification number will be generated when their data are stored into the database for the first time after the implementation of the system.

There is no such system which manages the medical data of each individual in the country. Existing systems store the data of only a particular organization or group of organizations but not all.

A.Objective of the work

a) Store vast amount of medical data
b) Efficient treatment through the data reference
c) Reduce the difficulties to keep the data safe
d) Easy Retrival of Patients details at any time.

B.Existing System

Cloud based health system's main focus is the patient's data collection, storage, access, analysis, and presentation etc.

II. RELATED WORK

Sawand, S. Djahel, Z. Zhang, and F. Naït-Abdesselam [1], The patient-centric health monitoring plays a vital role in e-healthcare service, involving a set of important operations ranging from medical data

collection and aggregation, data transmission and segregation, to data

The current patient data collection techniques are time consuming, inefficient, laborious. It is also obvious that currents technique is violating the real time data access for monitoring the patients.

In m-health care social networks, the personal health information is always shared among the patients located in respective social communities suffering from the same disease for mutual support, and across distributed health care providers equipped with their own cloud servers for medical consultant. However, it also brings about a series of challenges, especially how to ensure the security and privacy of the patient's personal health information from various attacks in the wireless communication channel such as eavesdropping and tampering.

C. Proposed System

Cloud based health system solution is based on the concept of "Cloud Computing" a distributed computing system where a pool of virtualized, dynamically-salable, managed computing power, storage, platforms, and services are delivered. This system provides an environment where patient's records are stored and it will be referenced by the doctors to improve the efficiency of the treatment.

This handles the medical history of each individual of the country and provides access to all registered hospitals to read or update the data. The hospital which accesses the database must be registered and must have got a license. The license number is used as a unique code to access the database. The details of the patients will be stored and an identification number will be generated when their data are stored into the database for the first time after the implementation of the system.

Whenever they go for a treatment, their medical data will be stored into the database using their identification number. For security reasons, any person who wants to view their data will be allowed only to read the data. They will not be given access to update the database. For hospitals to update the database they require the license number along with the identification number of the person whose record has to be store.

analytics. This survey paper firstly presents an architectural framework to describe the entire monitoring life cycle and highlight the essential service components. More detailed discussions are then devoted to at patient side, which we argue that it serves as fundamental basis in achieving robust, efficient, and secure health monitoring.

M. S. Shin, H. S. Jeon, Y. W. Ju, B. J. Lee, and S. P. Jeong [2], In today's era of aging society, people want to handle personal health care by themselves in everyday life. In particular, the evolution of medical and IT convergence technology and mobile smart devices has made it possible for people to gather information on their health status anytime and anywhere easily using biometric information acquisition devices. Healthcare information systems can contribute to the improvement of the nation's healthcare quality and the reduction of related cost. However, there are no perfect security models or mechanisms for healthcare service applications, and privacy information can therefore be leaked. In this paper, we examine security requirements related to privacy protection in u-healthcare service and propose an extended RBAC based security model. We propose and design u-healthcare service integration platform (u-HCSIP) applying RBAC security model. The proposed u-HCSIP performs four main functions: storing and exchanging personal health records (PHR), recommending meals and exercise, buying/selling private health information or experience, and managing personal health data using smart devices.

M. Rushanan, A. D. Rubin, D. F. Kune, and C. M. Swanson [4]. Balancing security, privacy, safety, and

utility is a necessity in the health care domain, in which implantable medical devices (IMDs) and body area networks (BANs) have made it possible to continuously and automatically manage and treat a number of health conditions. In this work, we survey publications aimed at improving security and privacy in IMDs and health-related BANs, providing clear definitions and a comprehensive overview of the problem space. We analyze common themes, categorize relevant results, and identify trends and directions for future research. We present a visual illustration of this analysis that shows the progression of IMD/BAN research and highlights emerging threats. We identify three broad research categories aimed at ensuring the security and privacy of the telemetry interface, software, and sensor interface layers and discuss challenges researchers face with respect to ensuring reproducibility of results. We find that while the security of the telemetry interface has received much attention in academia, the threat of software exploitation and the sensor interface layer deserve further attention. In addition, we observe that while the use of physiological values as a source of entropy for cryptographic keys holds some promise, a more rigorous assessment of the security and practicality of these schemes is required.

C. Bekara and M. Laurent-Maknavicius[7], The low-cost, unattended nature and the capability of self-organizing of sensors, yield the use of wireless sensor networks (WSN) very popular today. Unfortunately, the unshielded nature of sensors, their deployment in remote open (hostile) areas, and the use of wireless transmission medium, make them subject to several kinds of threats and attacks, like eavesdropping, intrusion, deny of services (DoS) attacks and nodes compromising. While most of threats and attacks can be prevented using cryptographic materials (i.e. shared pair- wise secret keys, certificates, etc.) provided by key management protocols, some other threats, like nodes replication attacks, can still go undetectable. Nodes replication attacks are harmful attacks, where an attacker compromising a node, uses its secret cryptographic key materials to successfully populate the network with several clones of it, in-order to gain the control over the network or disturb the normal operation of the network. Several nodes replication detection protocols were proposed in the literature, but unfortunately, they require either a high computation, transmission and energy overheads, or that nodes know their exact locations coordinates, which limits their usability in most WSN scenarios. In this paper, we present a new protocol for securing and preventing against nodes replication attacks in static WSN, which requires no knowledge of nodes deployment locations, and introduces no significant overhead on the resource-constrained sensors.

III. PROPOSED SYSTEM ANALYSIS AND MODULES

Cloud based health system solution is based on the concept of “Cloud Computing” a distributed computing system where a pool of virtualized, dynamically-salable, managed computing power, storage, platforms, and services are delivered. This system provides an environment where patient’s records are stored and it will be referenced by the doctors to improve the efficiency of the treatment.The Modules are

a) Admin Modules
b) Unique Id and Key verification
c) Reports Upload
d) Doctor Counseling
e) User Entry Checking
f) Database Report Search

A. Admin Module.

In this module, a User must Authorised in our application and there is a provider side must add the doctors and hospitals for the further counselling for Patients or Users. Even Doctor Profile, Doctors only able to known the Password for their view of Counselling Information.

b.Unique Id and Key verification.

In this module, when every provider must have a unique hospital details and doctor list. When a User comes under in an application and accepts the Provider for further Proceeding Comes under in the booked Provider alone.

c.Reports Upload.

In this module, when a User booked his Provider along with Hospitality Functions and Doctor Specialist in an application. Once a User come back for further Process They made counselling to Particular Doctor.

d.Doctor Counselling.

We consider the server to be semi-trusted, that means the server will try to find out as much secret information in the stored PHR files as possible, but they will honestly follow the protocol in general. On the other hand, some users will also try to access the files beyond their privileges. For example, a pharmacy may want to obtain the prescriptions of patients for marketing and boosting its profits.

e. User Entry Checking.

In this Module, we had implemented main goal of the Project it denotes security for viewing our personal information to all roles in an application. To prevent that we had proposed to use Attribute Based Encryption Algorithm for the access to encrypt the Selected Details to Restrict to view by others.

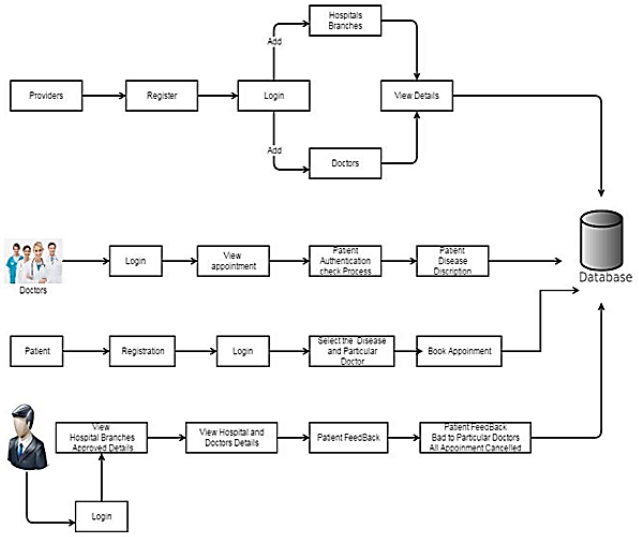
f. Database Report Search.

In this module, admin can able to view overall users report, Users personal Records and User Counselling Records. In Such Case user had made encrypted their information it will visualization in cipher text format.

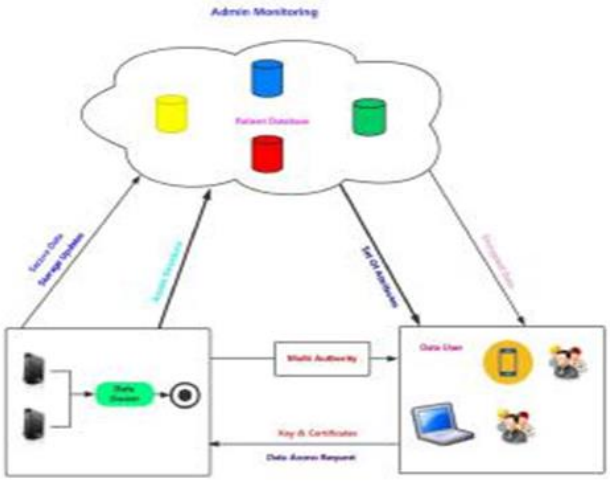
IV. FUNCTIONING AND IMPLEMENTATION

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The implementation stage involves careful planning, investigation of the existing system and its constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods. Data elements and data structures to be stored have been identified at analysis stage and are structured and put together to design the data storage and retrieval system.

a.Block Diagram:



b.Existing System Architecture:



In m-health care social networks, the personal health information is always shared among the patients located in respective social communities suffering from the same disease for mutual support, and across

distributed health care providers equipped with their own cloud servers for medical consultant. However, it also brings about a series of challenges, especially how to ensure the security and privacy of the patient's personal health information from various attacks in the wireless communication channel such as eavesdropping and tampering.

Disadvantage:

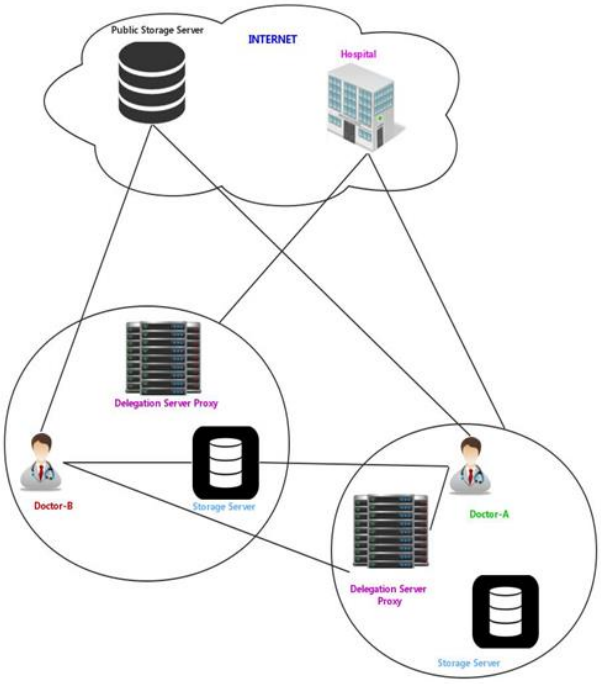
a) less security
b) Not straightforward
c) Various Attacks such as online and off attacks.
d) Inefficient
e) Time consuming
f) Laborious for the staffs

c.Proposed System Architecture

This system provides an environment where patient's records are stored and it will be referenced by the doctors to improve the efficiency of the treatment. This handles the medical history of each individual of the country and provides access to all registered hospitals to read or update the data. The hospital which accesses the database must be registered and must have got a license. The license number is used as a unique code to access the database. The details of the patients will be stored and an identification number will be generated when their data are stored into the database for the first time after the implementation of the system. Whenever they go for a treatment, their medical data will be stored into the database using their identification number. For security reasons, any person who wants to view their data will be allowed only to read the data. They will not be given access to update the database.

Advantage:

a) Achieving data confidentiality and identity privacy with high efficiency.
b) Efficiently realizing access control of patient's personal health information.
c) Resist various kinds of malicious attacks and far outperforms previous schemes in terms of storage, computational and communication overhead.



V. DATABASE DESIGN

A database is a collection of interrelated data stored with minimum redundancy to serve many users quickly and efficiently. The general Objectives of the database design are to make the data access easy, inexpensive and flexible to the design.

Data elements and data structures to be stored have been identified at analysis stage and are structured and put together to design the data storage and retrieval system user.

The data in the system has to be stored and retrieved from database. Designing the database is the part of system. The input of a system can be defined as the information that is provided to the system. This is used for future processing by the system to obtain meaningful information, which helps in decision-making. Input design is the process of converting user-oriented inputs to a computer-based format. Input is a part of overall system design, which

requires special attention. Inaccurate input data are the most common cause of errors in error processing. Input design can control errors entered by users. Entered data have to be checked for their accuracy and direction of errors. Appropriate error message have to be displayed. When an invalid data is entered, the user should not be allowed to type that data.

VI. CONCLUSION

In this work, proposed a system which monitors the health care details of each individual of the country. It comprises of modules like generating the unique ID and store and retrieve data of a person. The cloud computing is an emerging computing mode. It promises to increase the velocity with which applications are deployed, increase innovation, and lower costs, all while increasing business agility. The nature of cloud computing is useful for constructing the data center. To the new generation of cloud based health system, cloud computing is better approach in the future.

VII. FUTURE WORK

The need of an online certificate authority (CA) and one unique key encryption for each symmetric key k for data encryption at the portal of authorized physicians made the overhead of the construction grow linearly with size of the group. Furthermore, the anonymity level depends on the size of the anonymity set making the anonymous authentication impractical in specific surroundings where the patients are sparsely distributed.

VIII. REFERENCES

[1]. Sawand, S. Djahel, Z. Zhang, and F. Naït-Abdesselam, "Toward Energy-Efficient and Trustworthy eHealth Monitoring System, " China Commun., vol.12, no. 1, pp. 46-65, Jan. 2015.

[2]. M. S. Shin, H. S. Jeon, Y. W. Ju, B. J. Lee, and S. P. Jeong, "Constructing RBAC Based Security Model in u-Healthcare Service Platform," The Scientific World J., vol. 2015, Article ID 937914, 13 pages, http://dx.doi.org/10.1155/2015/937914, 2015.

[3]. C. Wang, B. Zhang, K. Ren, J. M. Roveda, C. W. Chen, and Z. Xu. "A Privacy-aware Cloud-assisted Healthcare Monitoring System via Compressive Sensing," in Proc. of 33rd IEEE INFOCOM, 2014, pp. 2130-2138.

[4]. M.Rushanan, A. D. Rubin, D. F. Kune, and C. M. Swanson, "SoK: Security and Privacy in Implantable

[5]. M. Rushanan, A. D. Rubin, D. F. Kune, and C. M. Swanson, "SoK: Security and Privacy in Implantable Medical Devices and Body Area Networks," in Proc. of

[6]. M.D.Mofjul Islam1, MD.Abdur Razzaque1 ,(senior member,IEEE), Mohammad Mehedi Hassan2,(Member ,IEEE),Walaa Nagy Ismail2, and Biao song2,(Member IEEE)," Mobile Cloud-based Big HealthCare Data Processing in Smart Cities" in proc of Computer Science, Digital Object Identifier 10.1109/ACCESS.2017.2707439.

[7]. C. Bekara and M. Laurent-Maknavicius, "A New Protocol for Securing Wireless Sensor Networks against Nodes Replication Attacks," in Proc. of 3rd IEEE Int. Conf. on Wireless and Mobile Computing, Networking and Communications (WiMOB 2007), 2007, pp. 59-59.

[8]. P. T. Sivasankar and M. Ramakrishnan, "Active key management scheme to avoid clone attack in wireless sensor network," in Proc. of 4th Int. Conf. on Computing, Communications and Networking Technologies (ICCCNT'13), 2013, pp. 1-4.

[9]. A. Marcos, J. Simplicio, H. I. Leonardo, M. B. Bruno, C. MB. C. Tereza, and M. N¨aslund, "SecourHealth: A Delay-Tolerant Security Framework for Mobile Health Data Collection," IEEE J. Biomedical a Health Informatics (IEEE Trans. INF TECHNOL B), vol. 19, no. 2, pp. 761-772, Mar. 2015.

[10]. R. X. Lu, X. D. Lin, and X. M. (Sherman) Shen, "SPOC: A Secure and Privacy-Preserving Opportunistic ComputingFrameworkforMobile-Healthcare Emergency," IEEE Trans. Parall. distr., vol. 24, no. 3, pp. 614-624, Mar. 2013.

[11]. A. Amirbekyan and V. Estivill-Castro, "A New Efficient Privacy-Preserving Scalar Product Protocol," in Proc. of Sixth Australasian Conf. Data Mining and Analytics (AusDM '07), 2007, pp. 209-214.

[12]. A. C. F. Chan, "Symmetric-Key Homomorphic Encryption for Encrypted Data Processing," in Proc. of 2009 IEEE International Conference on Communications (ICC '09), 2009, pp.1-5.

[13]. Imran A. Khan,"personalized electronic health record system for monitoring patients with chronic disease" NSPECAccessionNumber: 13614874 DOI: 10.1109/SIEDS.2013.6549505

[14]. Olga Boric-Lubecke,"E-healthcare: Remote monitoring, privacy, and security" INSPEC Accession Number: 14446855DOI: 10.1109/MWSYM.2014.68486 02 Publisher: IEEE 35th IEEE Symp. on Security and Privacy, 2014, pp. 524-539.

[15]. M. Jordanova, and F. Lievens, "Global Telemedicine and eHealth (A synopsis)," 20i i E-Health and Bioengineering Conference (EHB), pp. I-6, 24-26 Nov. 2011

[16]. I. Zheng, D. Simplot-Ryl, C. Bisdikian, and H. T. Mouftah, "The Internet of Things," IEEE Communications Magazine, 2011

[17]. D. Miorandi, S. Sicari, F. De Pellegrini, and Chlamtac, "Internet of things: Vision, applications and research challenges," Elsevier Ad Hoc Networks, 10 (2012), pp. 1497-1516

[18]. G. S. Andrews, "Los desaffos del proceso de envejecimiento en las sociedades de hoy y del futuro", En: Encuentro Latinoamericano y Caribeno sobre las Personas de Edad: ponencias presentadas al Seminario Técnico-LC/L, pp. 247-256, 2000.

[19]. E. V. Carrera, P. Morales, "ECG signal monitoring using networked mobile devices", Andean Region International Conference (ANDES-CON) 2012 VI. IEEE, pp. 35-38, 2012.

[20]. Hua-Pei Chiang, Chin-Feng Lai, Yueh-Min Huang, "A Green Cloud-assisted Health Monitoring Service on Wireless Body Area Networks", Information Sciences, vol. 28, pp. 118-129, 2014.

[21]. O. Banos, C. Villalonga, M. Damas, P. Gloesekoetter, H. Pomares, I. Rojas,PhysioDroid: combining wearable health sensors and mobile devices for a ubiquitous continuous and personal monitoring, vol. 2014, 2014.

[22]. B. Kayyali, D. Knott, S.V. Kuiken, The Big-data Revolution in US Health Care: Accelerating Value and Innovation, Mc Kinsey & Company, pp. 1-13, 2013.

[23]. Y.E. Gelogo, H. Kim, Integration of wearable monitoring device and android smartphone apps for u-healthcare monitoring system, vol. 9, no. 4, pp. 195-202, 2015.

[24]. Ying Zhang, Hannan Xiao, "Bluetooth-Based Sensor Networks for Remotely Monitoring the Physiological Signals of a Patient", IEEE TRANSACTIONS ON INFORMATION TECHNOLOGY IN BIOMEDICINE, vol. 13, no. 6, 2009.