

¹Rekha S.Dange
Vairagade

²Dr.Minakshi
Wanjari

An Approach Towards Standardization of Ehr with Efficient Accessibility of Data on Demand: A Review



Abstract: - Standardization of medical terminologies and the centralized electronic medical record (EMR) are the most addressed discussion in the healthcare industries. Patient master records and the treatment statistics records has wide spectrum and dynamic data structure. These records have high growth rate with huge volume over the period and which requires proper structured data base management system. Data science and the analytics could solve the problem of data management, but trust about data storage over the cloud may become major issue. These records may be archived for better storage management and could be replicated over multiple cloud or kept in a distributed manner for extended security. On other hand medical data generated through wearable medical devices or the portable devices used by home care patients may be connected to multiple cloud servers for better accessibility and security. Proposed system is to develop a generic medical record management system over multiple cloud and designing the Body Area Network (BAN) architecture connected to distributed cloud for data accessibility and security.

Keywords: BAN, EMR, IoMT, IoHT, ASTM, HL7

I. INTRODUCTION

Different medical devices viz. fixed ICU room machines and monitors, portable health data capturing devices are available in the market with proprietary firmware and communication techniques. With the rapid development in internet and remote device communication, more and more medical devices are connecting to each other for data exchange. Many laboratory equipment vendors adopted medical information exchange standards like ASTM or the HL7[1][2] These protocols have higher dependencies like physical connection and hence the logical configuration is avoided by portable devices and many basic or specific task medical equipment. Proposed invention or the idea is lightweight communication protocol architecture for medical devices with security and data communication over distributed cloud. This system enables different medical devices to create standard communication between machine to machine and machine to software. With right deployment, new device could also be able to communicate with existing devices. Idea is presented with proprietary hardware, standard communication method and system architecture.

The proposed System is based on the medical health record exchange between multiple software and hardware entities. This invention is the designing and deploying of the standard message passing structure and providing the security to communication between service provider and the entity. Entity may be the software, hardware or the firmware. This invention also focuses on stable and on time data availability at any point of time. This will help different entities communicate and manage the active connection over multiple cloud service provider levels.

As the global population is aging and people with chronic diseases are increasing, basic healthcare may become un-reachable to many people. Thanks to the Internet of Things (IoT) technique[3], it promotes the rapid development of e-health systems and makes healthcare easier for users who use portable devices. E-health is defined as an interdisciplinary subject which consists of public health, medical informatics and commerce. It can offer or enhance healthcare through the Internet using means like WiFi and 5G networks. E-health[4] systems bring users many benefits. They can save lives in emergency medical situations through the real-time monitoring of the connected devices. It is easy to detect the emergency such as asthma attacks, heart failure and diabetes. The medical data and health data will be collected through the connected devices. Then, the data is transferred to the doctor or the healthcare department by wireless network devices, such as mobile phones and tablets.

In fact, this data is a part of personal health records (PHRs)[5]. Data Collected by Smartphone PHR includes not

¹ Electronics and Telecommunication , G.H.Raisoni University, Amravati Email: rekhadange73@gmail.com

²Electronics and telecommunication Engineering Department, G. H. Raisoni College of Engineering, Nagpur Email: minakshi.wanjari@raisoni.net

only health data, but also some important information related to patient care. This data is managed by the patient and usually stored in the cloud server (medical servers). Unlike the electronic medical record, the PHR is not created and maintained by institutions such as medical establishments and hospitals. The patient does the data collection and uploading. The purpose of PHRs is to store an accurate and complete summary of the individual's medical history. They allow authorized users or institutions to access the data over the Internet. A recent survey shows that a majority of users use apps and

other tools to track their fitness, nutrition and sleep; 44 percent of people have accessed their medical records online. In a typical e-health personal health records (PHRs) architecture, the user's data are collected and sent to the medical servers. When the doctor needs to review the user's PHRs (medical data, medical record, etc.), he needs to download the PHRs from the medical server[6]. Nevertheless, the massive PHRs data are usually stored and processed in the cloud platform, such as Amazon Web Services, Google Cloud. Due to the fact that PHRs contain some sensitive and high-value data, the cloud server has become an attractive target for hacking.

II. LITERATURE REVIEW

The literature survey is mainly done on the basis of published articles and the research papers by the academic or medical researchers and the available existing protocols those are used for medical record exchange and standardization of the healthcare records.

A. Research and publication

Author[7]: Proposes a decentralized, interoperable trust model that suffuses Blockchains into healthcare IoHT. Blockchain technology provides a veritable platform to secure and enhance efficiency of healthcare-based internet of things (i.e. IoHT) framework. Author[8]: Authors have reported an effective cryptosystem aimed at securing the transmission of medical images in an Internet of Healthcare Things (IoHT) environment. The analysis part clearly proves that the system can be effectively used to encrypt medical images in IoHT framework. Author[9]: Healthcare monitoring framework based on the cloud environment and a big data analytics engine is proposed to precisely store and analyze healthcare data, and to improve the classification accuracy. The results show that the proposed model precisely handles heterogeneous data and improves the accuracy of health condition classification and drug side effect predictions. Author[10]: Proposes a novel method that combines knowledge-graph-based and word-embedding-based similarity measures via word entropy. The experimental results show that the proposed method achieves significant improvements over other word similarity measures in terms of the correlation coefficient. Author[11]: This work tries to provide a better and more efficient solution for securing all the health care data that are stored on the cloud, protect health care data from unauthorized access from an unknown source. Author[12]: Presents IoT Device for patient to measure various parameters that include emotions, mood variations, blood pressure, heart rate, skin temperature, and electrocardiogram. Solution is proposed to automate all the patient monitoring activities through Blue Eyes Technology. Author[13]: Proposes to develop a smart healthcare system in IoT environment and monitor patient's basic health signs and room conditions. The system is very useful in the case of infectious disease like a novel coronavirus. Author also proposes Healthchain, Secure EMRs Management and Trading in Distributed Healthcare Service System. Author[14]: Depicts Novel distributed data sharing scheme that applies the security benefits of blockchain. Proposed scheme also facilitates selective sharing of medical records among staff members that belong to different levels of a hierarchical institution. Author[15]: Proposes novel peer-to-peer EMRs data management and trading system. Health chain security analysis shows that healthchain can provide secure EMRs management and trading.

B. Existing protocols

In order to transfer the medical information or medical data exchange typically, following protocols are utilized through the software and the medical equipment.

1) *ASTM's*: Medical device and implant standards are instrumental in specifying and evaluating the design and performance requirements of a number of biomedical materials, tools, and equipments[1]. These apparatus are used in surgical procedures that involve the placement of such devices to specified parts and structures of the body (both humans and animals) for the purpose of enhancement or as an aid in a disability. These medical

device and implant standards allow material and product manufacturers, medical laboratories, and other concerned institutions to inspect and assess such instruments to ensure proper quality and workmanship.

2) *HL7*: Its members provide a framework (and related standards) for the exchange, integration, sharing, and retrieval of electronic health information. These standards define how information is packaged and communicated from one party to another, setting the language, structure and data types required for seamless integration between systems. HL7 standards support clinical practice and the management, delivery, and evaluation of health services, and are recognized as the most commonly used in the world.[16]

III. PROBLEM AREA

As a part of finding the research gap proposed system and existing system was studied to identify the need of the improvement area, lacking of functionality, and checking the interpretability of the different entities involved in the system. Following are the points or the lackunae found while studying and proposing the system.

1) In order to streamline the patient information including the profile, medical history, report, and the treatment needs to be recorded in uniform defined data format[17]. Here it has been found that there is no standardization of the data across all medical organization and healthcare department, So we have the scope to define the standard protocols for communication.

2) Different medical devices are generating the information related to detected condition, which may include the sensors or the machines[18]. Every machine generating the information in its own defined data format that needs to be standardized in order to make it available on same platform and could be understandable by individual system. Here we could say medical device are not interlinked or in sync with each other and needs to be designed with a capability to understand each others data.

3) Medical information needs to be paperless and in the form of softcopy to make it sharable between different service provider or the entities. This information maybe in different formats like tables, reports, pdfs, images hence need user specific centralized or distributed digital healthcare locker[19] to preserve and make it available as and when required to the user or the service provider. Functionality enhancement in any system may not be on the basis of need or the solution to real problem, those functionality could be for making the system easier, faster or enhancing the features. As a part of novel research, we need to find the base or foundation problem. Following is the base problem, which is kept in consideration while proposing and designing the system methodology. In current situation, patient might be operated or treated by multiple doctors or the hospitals over the years. This leads to non-maintenance of history of medical issues, treatments and medicines prescribed. This another issue needs a centralized patient medical history repository.

From the perspective of the scope of the proposed system, it could be utilized for multiple applications. The purpose of the proposed system is to design security framework, which could be generic but proposed system mainly focuses on medical healthcare records and application .

- Patient digital lockers for medical records management could be the next revolutionary product among citizen to manage centralized medical history and data.
- It will provide Easy access to medical history at multiple clinics and hospital due to which doctors or healthcare service provider make right decision about treatment to be given to patient on the basis of patient's previous records like allergies, long-term issues, specific diseases, etc.

IV. PROPOSED SYSTEM

The proposed system is based on the medical health record exchange between multiple software and hardware entities. This invention is for designing and deploying of the standard message passing structure and providing the security to communication between service provider and the entity. Entity may be the software, hardware or the firmware. This invention also focuses on stable and on time data availability at any point of time. This will help different entities communicate and manage the active connection over multiple cloud service provider levels.

Figure 1. illustrates the possible scope of data generated by the different entities of the proposed scope of work. All these entities generate the data related to central entity "patient" but the format generated by individual

entity or managed by service provider is in proprietary format and it has no standard method or format defined. Even the format managed by two different entities at same level or of same category may differ with respect to the data format. So the proposed system deals with the standardization of the medical healthcare information, so that individual entity can build an interconnection.

A. Data Communication standard protocol

Proposed healthcare communication protocol stack is made up of three main parts illustrated in figure 2. where, first part is security information layer consisting authentication information, second part is identity layer consisting device and identity information and third part is data layer consisting the healthcare related information.

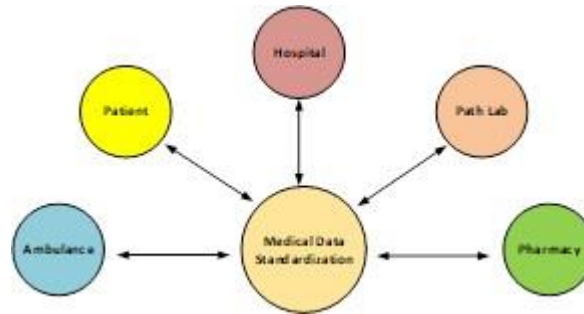


Figure. 1. Data standardization entities

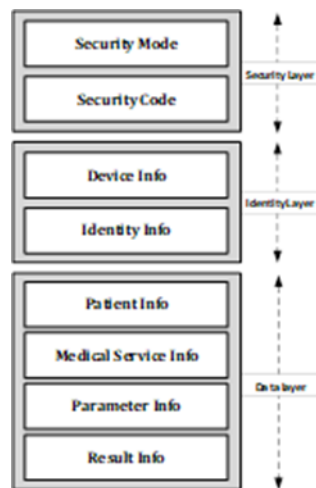


Figure. 2. Data standardization protocol stack

B. Security information layer stack

- Security mode consists of the possible mode of authentication and different possible security methods
- Security code or the encryption key required for thesecurity processing.

C. Message identity information layer stack

- Consists of device information that differ at different devices utilizing the communication protocol stack.
- Device identity information required for individual deviceunique identification and security check information.

D. Data layer stack

- Healthcare information (usually) related to patient, so this block consists of the patient information, if available.
- This block consists of the information related to medi-cal service information provided at multiple

level or at multiple sources.

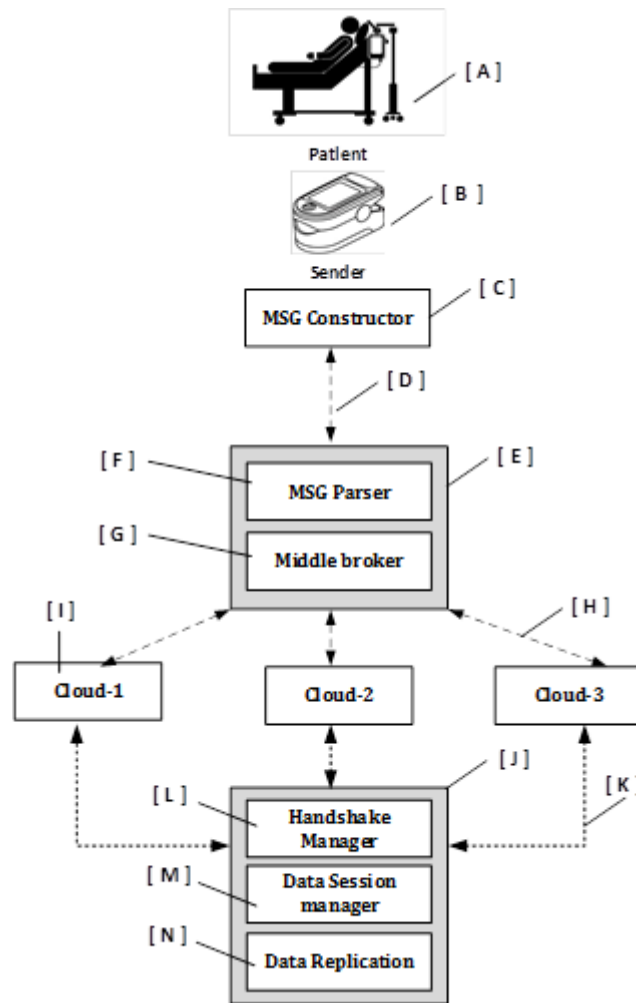


Figure 3. Proposed system workflow

- Healthcare information related to any affecting parameter under the associated service.
- This block consists of the result information (if any) associated with specified healthcare service.

Figure 3. illustrates the flow of communication and the sub-component involved into process.

[A] : Patient involved in a process is key of information stack.

[B] : Healthcare devices involved in process to fetch specific medical information.

[C] : While transferring or receiving the data it needs to construct the information in desired format.

[D] : Communication logical link/pipe used for data exchange between message constructor and the middle broker.

[E] : Middle broker block required for communication between actual devices and the cloud service provider.

[F] : Incoming message needs to parse into parts before transferring at multiple clouds and into multiple tokens.

[G] : Middle broker part is responsible for managing the data integrity and the data exchange between multiple cloud service providers.

[H] : Communication logical link/pipe used for data exchange between middle broker and the cloud service provider.

[I] : Final entity responsible for storing the final data or providing software as service. Single cloud or the multiple cloud service provider can be the part of the array of independent cloud.

[J] : Load balancer block, this is responsible for handling the load and the data sharing or storing between multiple cloud service providers. This block consists of multiple internal blocks to handle the execution and the process.

[K] : Communication logical link/pipe used for data exchange between middle broker and the cloud service provider.

[L] : Handshake manager looks at the communication establishment and the communication stability part. This will keep the watch on communication and connectivity availability part of interconnection between multiple cloud service providers.

[M] : This block will handle the switching of active session between multiple cloud service providers. This will handle transferring the active session from one service provider to another in case of failure of any service provider. This will take care of no data loss in active session.

[N] : This block will be responsible for replicating the data at multiple location in case of failure of any of the service providers. It may also help in data recovery in case of hardware or the system failure.

V. CONCLUSION

Proposed research work is mainly targeted to work towards creating centralized command integration gateway for better medical assistance system. Study involves designing and developing feasible portable diagnostics system and centralized data exchange gateway with record storage for critical healthcare support. The project consist of sensors, which will be merged to form a single system of sensors for measuring health parameters. The data will be transferred to the cloud with security and can be analyzed by the medical practitioner for timely treatment. It will not only reduce the stress of hospital visits, medical bills, and multiple diagnoses, but also predict the possibility of severe diseases beforehand, which could save lives.

Since the proposed system would be a combination of different products, there is a need to standardize the communication model. For this purpose, there is a need of large support for deployment and acceptance at multiple level of authorities. Different vendors may reject the proposal as it may lead them to losses in new product development. Secondly, experts need to work out on the privacy and the security concern of every device user. The proposed framework must be strong and feasible from working perspectives.

REFERENCES

- [1] M. A. Skoog, L. R. Hook, and W. Ryan, "Leveraging astm industry standard f3269-17 for providing safe operations of a highly autonomous aircraft," in *2020 IEEE Aerospace Conference*. IEEE, 2020, pp. 1–7.
- [2] T. M. Alenazi and A. A. Alhamed, "A middleware to support hl7 standards for the integration between healthcare applications," in *2015 International Conference on Healthcare Informatics*. IEEE, 2015, pp. 509–512.
- [3] C. Priya *et al.*, "Enabling the efficiency of blockchain technology in tele-healthcare with enhanced emr," in *2020 International Conference on Computer Science, Engineering and Applications (ICCSEA)*. IEEE, 2020, pp. 1–6.
- [4] H. T. Yew, M. F. Ng, S. Z. Ping, S. K. Chung, A. Chekima, and J. A. Dargham, "Iot based real-time remote patient monitoring system," in *2020 16th IEEE International Colloquium on Signal Processing & Its Applications (CSPA)*. IEEE, 2020, pp. 176–179.
- [5] A. Yoshitaka, S. Chujyou, and H. Kato, "Analysis and design of personal health record management system," in *2013 International Conference on Signal-Image Technology & Internet-Based Systems*. IEEE, 2013, pp. 800–805.
- [6] Y. Zhang, D. He, M. S. Obaidat, P. Vijayakumar, and K.-F. Hsiao, "Efficient identity-based distributed decryption scheme for electronic personal health record sharing system," *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 2, pp. 384–395, 2020.

- [7] E. M. Abou-Nassar, A. M. Iiyasu, P. M. El-Kafrawy, O.-Y. Song, A. K. Bashir, and A. A. Abd El-Latif, "Distrust chain: towards blockchain- based trust models for sustainable healthcare iot systems," *IEEE Access*, vol. 8, pp. 111 223–111 238, 2020.
- [8] N. Tsafack, S. Sankar, B. Abd-El-Atty, J. Kengne, K. Jithin, A. Belazi, Mehmood, A. K. Bashir, O.-Y. Song, and A. A. Abd El-Latif, "Anew chaotic map with dynamic analysis and encryption application in internet of health things," *IEEE Access*, vol. 8, pp. 137 731–137 744, 2020.
- [9] F. Ali, S. El-Sappagh, S. R. Islam, A. Ali, M. Attique, M. Imran, and K.- S. Kwak, "An intelligent healthcare monitoring framework using wear- able sensors and social networking data," *Future Generation Computer Systems*, vol. 114, pp. 23–43, 2021.
- [10] D. Zhang, X. Xia, Y. Yang, P. Yang, C. Xie, M. Cui, and Q. Liu, "A novel word similarity measure method for iot-enabled healthcare applications," *Future Generation Computer Systems*, vol. 114, pp. 209–218, 2021.
- [11] U. Kumar, R. K. Pathak, and A. Kumar, "Handling secure healthcare data streaming using r2e algorithm," in *2020 International Conference on Electronics and Sustainable Communication Systems (ICESC)*. IEEE, 2020, pp. 732–737.
- [12] K. Dhinakaran, M. Nivetha, N. Duraimurugan, and D. J. W. Wise, "Cloud based smart healthcare management system using blue eyes technology," in *2020 International Conference on Electronics and Sustainable Communication Systems (ICESC)*. IEEE, 2020, pp. 409–414.
- [13] E. Zaghoul, T. Li, M. Mutka, and J. Ren, "d-mabe: Distributed multilevel attribute-based emr management and applications," *IEEE Transactions on Services Computing*, 2020.
- [14] C. Li, M. Dong, J. Li, G. Xu, X. Chen, and K. Ota, "Healthchain: Secure emrs management and trading in distributed healthcare service system," *IEEE Internet of Things Journal*, vol. 8, no. 9, pp. 7192–7202, 2020.
- [15] A. A. Corici, R. Olaf, B. Kraufmann, A. Billig, J. Caumanns, M. Deglmann, V. Walter, J. Rixin, and G. Nolte, "Interoperable and discrete ehealth data exchange between hospital and patient," in *2020 23rd Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN)*. IEEE, 2020, pp. 168–170.
- [16] E. Asare, L. Wang, and X. Fang, "Conformance checking: Workflow of hospitals and workflow of open-source emrs," *IEEE Access*, vol. 8, pp. 139 546–139 566, 2020.
- [17] M. Ianculescu, A. Alexandru, G. Neagu, and F. Pop, "Microservice- based approach to enforce an ioht oriented architecture," in *2019 E- Health and Bioengineering Conference (EHB)*. IEEE, 2019, pp. 1–4.
- [18] S. Tonello, M. Borghetti, E. Sardini, and M. Serpelloni, "Improved portable measuring device for real-time humidity and temperature monitoring in intensive care unit," *IEEE Instrumentation & Measurement Magazine*, vol. 23, no. 4, pp. 79–86, 2020.
- [19] D. Sparrell, "Cyber-safety in healthcare iot," in *2019 ITU Kaleidoscope: ICT for Health: Networks, Standards and Innovation (ITU K)*. IEEE, 2019, pp. 1–8.