AN EFFECTUAL DATA MANAGEMENT OVER HEALTHCARE SYSTEMS FOR IMPROVING PRIVACY IN IoT ENVIRONMENT

K. Krishna Prasad¹*, P. S. Aithal² and A. Jayanthiladevi³

¹Post-Doctoral Fellow & Associate Professor-Computer Science & Information Science, Srinivas University, Karnataka, India
²Vice-Chancellor-Srinivas University, Karnataka, India
³Post-Doctoral Fellow & Professor-Computer Science & Information Science, Srinivas University, Karnataka, India
*Corresponding author e-mail: krishnaprasadkcci@srinivasuniversity.edu.in

Abstract. The advancements in hardware and networking technology are merged with Internet of Things (IoT) which provides flexibility for monitoring the health condition of individuals. This is a smart environment that includes city, homes, and agriculture; as well, it recently includes healthcare systems for disease prediction and for medical advices. To improve the ability of IoT with healthcare system, the layers of data transmission has to be analyzed. This is to validate the faster response of physicians during the time of communication and lower latency. Moreover, this technology encounters various challenges in providing privacy towards the users and to address this privacy issue to certain extent. In the initial stage, the technology runs with a lesser privacy. Hence, this work deals with the modeling of e-healthcare framework that deals with preserving electronic medical records and attempts to eliminate privacy issue. However, the experimentation is done with MATLAB environment that concentrates on the metrics like response time and delay. The anticipated model provides better outcome in contrary to other models. The outcomes of this work are effectual while offering privacy with standardized network factors.

Keywords- Healthcare, latency, privacy, medical records, communication

1. Introduction
The recent advancements in digital processing and networking technologies have provided the way for handling the emergency conditions by giving online services. These services make use of Internet of Things (IoT) as a platform to connect with the process, people and the things [1]. Therefore, fulfilling the comfort towards social life of humans is very important [2]. These services make researchers and technologies to move from centralized environment to distributed environment. As an outcome, the smart homes, wearable devices, cities, mobility and healthcare are emerging technologies recently [3]. Subsequently, the present internet technology and its services are improved with the data technology for device proliferation, and it produces huge amount of data. Amazon, Cisco, Microsoft, Google and some other leading Information Technology (IT) industries are deployed with Data Centers (DC) for...
storing and computing the generated data with diverse application and services with paid-usage mode [4]. Even though, this model is resourceful as per its usage, however it is applicable for latency with finest suit for real-time applications [5].

With the recent usage and accumulation of data, 92% data forecasting with workload is identified and urged with the deployment of control layers over computing environment nearer to the end-to-end devices to assist data locality and mobility [6]. However, the term computing is anticipated by Cisco in 2012 and this domain receives better attention for diverse application by academia, researchers, and industries [7]. The ultimate objective for deployment is to take benefits over the end-devices and at the edge the devices are completely provided with diverse resources like bandwidth, computation, and storage for processing the real-time data connected with neighboring nodes in one-hop transmission with reduced delay [8]. The fog and cloud computing are benefitted mutually and inter-dependent with one another. It is known that the cloud coordination with the successive nodes is handled by diverse heavyweight data [9]. For making comparison, the delay sensitive data is processed with the use of fog nodes in IoT based proximity with end devices.

As discussed previously, IoT provides an open door for handling e-health and other various application which turns to be significant and immense important task to be accomplished by recent investigators. The healthcare system relies over the radio frequency based on ubiquitous functionality and wireless networking technology. Diverse smaller actuators and sensors are placed over the human body and interconnected with other devices for data accumulation [9]. The data is generated with the use of actuators and sensors are stored which is utilized by the medical consultant and other physicians during the emergency conditions. For instance, the first tele-robotic surgery is carried out over the patients from some other remote location with the use of robotically controlled instruments. The pharmaceutical and medical researchers also need the patient’s record for performing the research task. The current advancements in cloud and IoT technologies have the ability to improve the e-healthcare services [10]. Moreover, the retrieval and storage of these sensitive health care records are termed as Electronic Medical Record from cloud the hold huge privacy concern based factors specifically to recognize the patients.

![Figure 1. Generic view of IoT devices in healthcare devices (Source: Zhang et al., 2018)](image)

The data privacy is based on four different types: 1) personal information based privacy that refers to data privacy; ii) personal behavior based privacy; iii) personal communication based privacy and iv) individuals' privacy. The privacy toward the EMR cloud data should be compromised and deliberated and therefore the data disclosure is more beneficial for attackers and harms the users. Diverse techniques are considered to resolve this issue over the cloud privacy. The trusted computing, encryption techniques, effectual private information, intention hiding approaches are some tested techniques. However, the huge amount of data and the process of attaining mis-management with cost factors, query support constraints, computational overheads and inappropriate key usage. Henceforth, the mechanism development is utilized for handling the EMRs devoid of exposing the identities or privacies with appropriate access control techniques are needed for certain time period.
The rest of this work is partitioned as: Section 2 is related works; Section 3 includes methodology; section 4 is results with discussion; section 5 includes conclusion with future research directions.

2. Related works
Con conventionally, the centralized data management with cloud computing is examined in various health care systems. Author in [11], anticipated a centralized CC platform that facilitates the physicians to observe the patients and share the healthcare information with some confidentiality. Some other works like [12], concentrates on the use of cloud platform to process, collect and store the information in a unified format. This platform is considered as a completely central authority and trusted environment for all network entities. Subsequently, author in [13], concentrates in semi-trusted CC model and pretends to apply attribute-based encryption model for attaining fine-grained access control with data and eliminate privacy exposure for unauthorized parties. Specifically, various authorities are used for governing successive user subset for role attributes.

Moreover, some works like [14], gives more attention for modeling block-chain based access control for enhancing medical records migration towards cloud-based platforms. Specifically, the progressive block-chain technology was used for facilitating the EMR access towards the identity of membership and verification authentication. Subsequently, data sharing was executed with lesser overheads, scalability and privacy protection. Some works like [15], concentrated on certain block chain nodes and some normal nodes with veto power and voting rights correspondingly. They jointly show the determination of uploading the healthcare data which is acceptable and valid. The objective is to fulfill the modifications towards the prevailing healthcare data that are traced and validated. However, certain prototype is executed with block chain based systems successively like MedRec and contract based clinical trials.

By multiple edge server scheduling process, the authorization established collaboratively to deal with the network based healthcare data in a completely decentralized manner. The task managing is achieved by on-demand secure provisions. In edge computing, the complex processing of this procedure is dealt with the healthcare data that is shifted with edge servers. However, the supervised access control is easily facilitated for facilitating external entities, for instance, data miners and healthcare service providers for accessing healthcare based data with higher security considerations.

For authorized data access to healthcare data, the miners pretend to run huge data mining algorithms with edge servers. The server exploitation is resourceful to deal with execution time and to improve the accuracy of data rate in mining process. With the negotiation of users with data trading, the appropriate decision making towards data miners capability is improved with renting proxy servers are to assist interactions with users.

3. Methodology
This section discusses about the E2E architecture of IoT platform for providing solution to healthcare system. This system comprises of four modules like sensing, transmission and layers based transmission as in Fig. 2. The former later comprises of certain network devices and sensors concentrates in the health information for processing and transferring data to successive layers. These devices constantly observe the parameters like temperature, blood pressure, heart rate and other parameters. The sensors are accountable for data transmission, and notifications to carry out necessary actions.

The communication layers comprises of number of connected nodes termed as edges that are accountable for data reception from sensors to IoT devices and process them locally, examine it and examine the health care patterns and report it to them. The edges show communication, storage, processing, and controlling units to acquire lesser delay. The communication module works as interface among the connectivity components over all the layers of communication. The controllers are used for transferring data from sensors to other and forward it to successive layers. The storage unit is nothing but huge database systems that can hold massive amount of data for shorter time period.
To attain better scalability, it is necessary to assist diverse kinds of connection components. This needs support to other network protocols for both wireless/wired connections among the network. The communication module is accountable for handling security and data along with the crucial issues to networked systems among the end systems. There are certain systems that are considered to eliminate attacks. The DC is executed over this layer that provides promising outcomes like holding the healthcare data repositories. The database comprises of three features like integration with other devices, data analysis and decision making system with medical practitioners and other parties. The data comprises of analysis with diseases for prior prediction. This is achieved with the database system like relational database that are adopted for various system levels.

**Fig 2: IoT layers for communication**

The architectural model of the anticipated model is given in Fig. 3. There are certain services provided by the healthcare systems like medical record management services and healthcare monitoring. This system is designed and organized as sub-systems. The components are deployed with overall design model specifically for sensing and storing. The IoT device gathers the healthcare data and forwards it to edge devices for data prediction and analysis. The reports are given to patients through PC, mobile or tablet. This unit is accountable for offering certain medical services to patients through data storage system to store and retrieve medical information. This system is responsible for processing and analyzing health data and mining to offer needed information.

**Figure 3. Architectural model**
For constructing a complete end system, diverse data structures are produced with appropriate flow over the considered system. This system comprises of various IoT devices, where sensors are connected with heterogeneous environment. The device can process and store huge data to facilitate system for delivering services with terminal parts. The centralized database is used for storing data and assists in decision making. The system is not provided for simple application which is used in certain location. This system comprises of distributed system that are merged with other devices. The sub-system deals with certain healthcare data devoid of acquiring access with centralized information.

The database aims in analyzing and collecting data with high efficiency. Subsequently, it is essential to adopt flexible data to conventional database format. This system is more dynamic. The model is required for handling machine generating system. The characteristics are assisted with the system executed by device implementation. The healthcare information is gathered from various systems for monitoring the devices and the partial data is needed for the device units to carry out processing and making appropriate decisions. The end device receives huge amount of network data to storage and retrieve data for making further decisions. There are diverse benefits with relational data where its ability and robustness to deal with huge data. The medications and scan reports are not provided very frequently. The aim is to store and retrieve data from health records. The records comprises of historical attributes to diagnose the disease. This system holds medical information from diverse sources like device sensors, address, personal information, progressive notes, and lab reports, past history and family histories.

It is noted that diverse information are used for multiple formats and structures. Therefore, it is not accountable to distribute data to electronic records as dynamic schemes. Then, the data is migrated and centralized with data storage. The database requires the ability to interchange and merge data among the data schemes to the edge devices. This assists in updating the information and adequately supports in decision making with diverse sources over the networks. The strategies used for data construction holds the comprehensive medical records. The hospitals comprises of various departments. These departments provide information for transmission. Subsequently, some general health information offer services like elderly services, tumors and treatment process. There are certain units that prevail over the hospital to serve various kinds like pharmacy, laboratory and radiology.

The basic concern towards the data is to eliminate privacy violations and provide appropriate solutions when handling the individual data to miners. The users take appropriate data to grant access for privileges. The sensitive information requires privacy preservation. The sensitive information towards healthcare data comprises of users name, ID, and communication details. Recently, the data anonymity is extensively applied to eliminate or modify identifiers. The sensitive information is achieved with privacy preservations. It collects intersecting data from users for carrying out mining tasks. It is acquired from data collection over the network and distributes it to servers to eliminate users for performing data trading in every region. This promotes decentralized data. It needs rewards from local users with incentive. This incentive is eliminating potential risks in privacy and economic to stimulate users.

Based on these principles, the decentralized data among the miners and users is provided with the use of servers. The trusted server acts as a broker for mining data and realizes the request from collected data. The server assists in providing appropriate ownership for the data. Subsequently, the users deal with the server to eliminate unauthorized access and to carry out data modification before publishing data to mining. The server notifies data holders regarding data request by communicating with the users proximally. The servers assist in transmitting reward policy to data owners. At last, the data is gathered from edge servers. The miner allocates the server for mining and tasks the results from individual servers. The servers are crucial for coordinating decentralized data among the users and miners with proper care.

4. Numerical results
Here, simulation has been done with MATLAB simulation environment by constructing a private cloud to make appropriate replication function and for executing privacy based modeling. File availability, replication and limitation related to data replication. Mathematical modeling of data replication is anticipated here. Table I depicts simulation setup of proposed model.
Table 1. Parameter setup

| Parameter               | values          |
|-------------------------|-----------------|
| Total DC                | 1               |
| Cost                    | 500             |
| MIPS                    | 2000            |
| Bandwidth               | 5-10 GB         |
| Total VM                | 200             |
| RAM                     | 02 GB           |
| Cloudlet                | 1000 task       |
| Task length             | 2000            |
| Total files             | 3               |
| Cost based replication  | 500             |
| Total users             | 50              |

Figure 4. Delay tolerance

Figure 5. Energy consumption based cost estimation
**Figure 6.** Energy efficiency in Scenario 2

**Figure 7.** Total data transmission rate

**Figure 8.** Cost replication
Fig 4 depicts the delay tolerance of the IoT devices for retrieving data from the source. The anticipated model has the ability to deal with delay. Fig 5 depicts the energy consumption of the devices along with the cost estimation. Fig 6 depicts the energy efficiency of the node connectivity with the end devices. Fig 7 demonstrates the data transmission rate of the node from source to destination (E2E) devices. The cost replication of this model is comparatively lesser than the prevailing approaches. This model pretends to boost the privacy by eliminating the violations. The attackers make the user to violate the rule and dissolve the privacy and security factors. Fig 8 depicts the average job performed over the devices and the total completed tasks from the network model. The anticipated model gives better trade-off in contrast to other models.

5. Conclusion
The anticipated model for healthcare system is to offer privacy over the data stored in cloud environment with the use of IoT technologies. The requirements for maintaining the privacy with healthcare data is secrecy, energy efficiency, transmission rate and cost. This healthcare model provides superior QoS requirements like lesser overhead and lesser bandwidth utilization, reduced delay and service availability. The anticipated model helps to enhance the multi-cast communication over the network environment with diverse privacy providing factors and reduces the packet drops by constantly monitoring the layers of communication environment. This model offers secure healthcare communication. In recent times, it is generally surgical processes that are monitored by the physicians remotely. With this condition may harm the patients under treatment, when it moves to distributed environment. Therefore, the anticipated model is more compatible with the available layer monitoring and offers a faster and secure accessibility over patients’ data with higher reliability and accuracy with healthcare and information system. In future, the process optimization is considered for validating the global solutions for measuring data transmission with IoT.

REFERENCES

[1] A. Al-Fuqaha, M. Guizani et al., “Internet of things: A survey on enabling technologies, protocols, and applications,” IEEE Commun. Surveys Tuts., vol. 17, no. 4, pp. 2347–2376, Oct.- Dec. 2015.
[2] H. Zhang, J. Li, B. Wen, Y. Xun, and J. Liu, “Connecting intelligent things in smart hospitals using NB-IoT,” IEEE Internet Things J., vol. 5, no. 3, pp. 1550–1560, Jun. 2018.

[3] Z. Su, Y. Hui, Q. Xu, T. Yang, J. Liu, and Y. Jia, “An edge caching scheme to distribute content in vehicular networks,” IEEE Trans. Veh. Technol., vol. 67, no. 6, pp. 5346–5356, Jun. 2018.

[4] Z. Su, Y. Wang, Q. Xu, M. Fei, Y. Tian, and N. Zhang, “A secure charging scheme for electric vehicles with smart communities in energy blockchain,” IEEE Internet Things J., pp. 1–1, 2018.

[5] H. Zhang, J. Liu, R. Li, and H. Le, “Fault diagnosis of body sensor networks using hidden markov model,” Peer-to-Peer Netw. Appl., vol. 10, no. 6, pp. 1285–1298, 2017.

[6] H. Zhang, J. Liu, and N. Kato, “Threshold tuning-based wearable sensor fault detection for reliable medical monitoring using bayesian network model,” IEEE Syst. J., vol. 12, no. 2, pp. 1886–1896, Jun. 2018.

[7] C. Yi, Z. Zhao, J. Cai, R. L. de Faria, and G. M. Zhang, “Priority-aware pricing-based capacity sharing scheme for beyond-wireless body area networks,” Comput. Netw., vol. 98, pp. 29–43, 2016.

[8] C. Yi, A. S. Alfa, and J. Cai, “An incentive-compatible mechanism for transmission scheduling of delay-sensitive medical packets in e-health networks,” IEEE Trans. Mobile Comput., vol. 15, no. 10, pp. 2424–2436, Oct. 2016.

[9] G. Yang, L. Xie et al., “A health-IoT platform based on the integration of intelligent packaging, unobtrusive bio-sensor, and intelligent medicine box,” IEEE Trans. Ind. Informat., vol. 10, no. 4, pp. 2180–2191, Nov. 2014.

[10] Z. Liu, B. Liu, C. Chen, and C. W. Chen, “Energy-efficient resource allocation with QoS support in wireless body area networks,” in Proc. IEEE GLOBECOM, Dec. 2015, pp. 1–6.

[11] C. Yi, S. Huang, and J. Cai, “An incentive mechanism integrating joint power, channel and link management for social-aware D2D content sharing and proactive caching,” IEEE Trans. Mobile Comput., vol. 17, no. 4, pp. 789–802, Apr. 2018.

[12] C. Yi, J. Cai, and G. Zhang, “Spectrum auction for differential secondary wireless service provisioning with time-dependent valuation information,” IEEE Trans. Wireless Commun., vol. 16, no. 1, pp. 206–220, Jan. 2017.

[13] Chang, H.-T., & Lin, T.-H. (2016). A Database as a Service for the Healthcare System to Store Physiological Signal Data. PLoS ONE, 11(12). doi:10.1371/journal.pone.0168935

[14] Juliana C., Adrian B., Margaret Allman F.: ‘A study to determine the most popular lifestyle smartphone applications and willingness of the public to share their personal data for health research’, Telemed. E-Health, 2016, 22, (8), pp. 655–665

[15] Luna R., Rhine E., Myhra M., ET AL.: ‘Cyber threats to health information systems: a systematic review’, Technol. Healthc., 2016, 24, (1), pp. 1–9