http://dx.doi.org/10.21172/ijiet.123.03

Extensive Study Of Iot In Healthcare Based On Machine Learning And Cloud

Asmita Bhowal[1]
[1]*Department of Information Technology, Netaji Subhash Engineering College, Kolkata, West Bengal, India*

Abstract- IoT is one of the recent attractions in the world of healthcare. The modern healthcare system and IoT has brought benefits to both physicians and patients, since they can be applied to various medical areas such as real-time monitoring, patient information management, and healthcare management. There are also systems that uses machine learning and cloud computing technologies for better data processing and storage that has been mentioned in the paper. However with the progress of IoT in healthcare, one of the main concerns is security and privacy as the data generated from the E-health systems can be accessed by a variety of users. So in this paper, the threats faced by the healthcare system has been mentioned along with a proposed architecture that uses the concept of Intrusion detection system.
Keywords – Internet of Things, E-Healthcare, machine learning, cloud computing.

I. INTRODUCTION

In the modern era of twenty first century, IoT has become an integral part of our everyday lives. Starting from Smart Home, Smart grids and connected cars to Industrial Internet, IoT also has a lot of applications in the field of healthcare. Healthcare is one of the basic needs in human life but with a growing population and the number of diseases increasing every day, the cost of healthcare services is also sky high. Under such circumstances, the advancement of IoT has opened up a new path in the healthcare industry that can help discover new treatment methods. Iot has made it possible for people to provide and receive healthcare services across a series of interconnected networks and Iot devices which is explained clearly in [1]. This paper provides an extensive literature survey on the different types of models proposed by researchers over the years involving machine learning and cloud computing in IoT-healthcare. It also gives an extensive study of the various security issues faced in IoT-healthcare. Further the paper also has an in-depth description of the proposed model architecture.

The rest of the paper is organized as follows. Extensive literature survey has been provided in section II. Proposed Architecture is explained in section III. Concluding remarks are given in section IV.

II. EXTENSIVE LITERATURE SURVEY

Many researchers have proposed models to use machine learning algorithms in IoT-healthcare systems.

2.1 Machine Learning in Healthcare

In [2], the main focus is on increasing developments in areas of wireless communications for low power sensor devices like WBANs (Wireless Body Area Networks). The proposed model makes use of mobile technology to form a cloud based WBAN framework that help to monitor patients in their real time environment. The system work by creating records of patient's data so that their respective healthcare providers can use the data to check their patient's condition whenever required.

Machine learning techniques like feature selection and classification techniques are then used for advanced processing of the data sent from the smartphone. The information generated after the advanced processing is either stored or sent to the respective doctor. The main problem in this system is the direct dependency on smartphones which has a small battery life. If instead of any kind of processing in a smartphone, the raw data can be directly sent to the cloud for complete processing, then the system would have been more useful. The other area of problem is that the information obtained from the cloud, instead of being further analyzed is directly sent to a doctor who manually analyzes the result. If some classification algorithms can be implemented like send an alert to the healthcare practitioner in case an abnormal reading in the patient's data is detected, then this can provide additional help to the doctor and also help analyze the patient's condition faster.

In [3], a system has been designed for big data application with the aim of monitoring the emotional states of patient. Big data management is an important part in this system, as the system aims to draw links between emotional responses and physiological changes to see how the physical condition changes depending on the patient's emotional state. As a result, a large amount of patient's data gets accumulated on the cloud which requires efficient data mining techniques for extraction of required information. Here the primary focus of the cloud storage is not only to maintain the patient's health record but also apply an efficient machine learning algorithm in order to maintain such huge data sets.

The use of machine learning algorithms for big data management can be seen in [4]. This work makes use of MapReduce parallel processing framework to provide a scalable and fault tolerant cloud architecture for huge data processing. This framework has the ability to process the large volume of data in parallel on a cloud and help in big data analysis. The proposed model mentioned in this work, uses a window based model for temporary data collection in order to enhance patient health monitoring. The patient's physiological condition are collected for different time frames. This is particularly beneficial for time series patient who require self monitoring. This method supports the storage and information retrieval over the time stamp. Also the physiological parameters and frequency of medical visits are both stored in the patient's health record and all this information is used to find interrelationship between the patients having different health parameters and disease using Intra-cluster and Inter-cluster analysis, under the MapReduce parallel processing framework. Further the model exploits Hidden Markov Model and Viterbi algorithm for future health condition prediction. It was observed that the model showed 98% accuracy in predicting the future health status of the patients. The only area of concern in the work is whether the cloud storage model will still hold even when the data increases over time and the database becomes non static and may keep on expanding.

As machine learning became more and more popular in conducting healthcare systems, in the past few years many researchers compared the machine learning algorithms used in different fields of IoT and healthcare and which are more efficient than the others. One such comparison can be observed in [5]. In this work, the research is not only limited to basic machine learning algorithms but further delves into the concept of deep learning. Deep Neural Networks has been compared to Gradient Boosting Decision Tree, logistic regression and support vector machine algorithm for predicting stroke based on a dataset obtained from a large scale population database. The work showed that Deep Neural Networks has an accuracy of 87.3% while the others were almost similar in performance except SVMs. The support vector machines showed the worst accuracy out of all the algorithms. Thus this clearly shows that Deep Neural Networks are the most suitable while SVMs are the least suitable. Even though Deep Neural Networks were proved to be the best algorithm but still it is more complex than the rest, so before using it in real life, one needs to consider the complexity of the algorithm.

In [6] multiple regression techniques have been used to manually create a cause and effect model for psychological health of patients. The authors have used the responses from a survey and used it to form a relationship between psychological wellness and survey responses. Machine learning algorithms like multi-layer perceptron (MLP), SVMs for regression (SVR), generalized regression neural networks (GRNN), and k-nearest neighbour (kNN) regression approaches were compared for determining a person's psychological wellness index based on five key parameters of psychological health.

2.2 Security in Health Care

A comprehensive survey of IoT health care systems is given in [7]. It provides an in depth study about security requirements and the challenges faced by IoT security. The patient always want their data to be secured. In the end everyone wants their data to be not accessed by unauthorized users, protected during adversaries, data integrity to be conserved, mobility, scalability, non repudiation of data, fault tolerance, security updates etc. These are the basic requirements that are expected to be executed effortlessly by an efficient E-health system. The authors describe how there is always a chance of threat attack from both within and outside the network. As a result, they have focused their study on an attack taxonomy which shows different kinds of attacks faced in different areas of security. They have divided existing and potential threats based on the basis of information-, host-, and network-specific compromise.

The paper provides a collaborative security model to reduce the security issues across the health care systems. The security model has been designed with dynamic properties in order to accommodate future unseen threats and attacks. The model clearly depicts what happens when a new kind of threat occurs. The existing model becomes inefficient to ward off such attacks. As a result there is need of dynamic algorithms to deal with these unpredictable situations. The model provides a way for strong collaboration between services so that the effects due to present, possible and unseen attacks can be reduced and eliminated. Also, it shows the impact of big data, ambient intelligence and wearables across various E-Health contexts. It provides policies and regulations to improve IoT-based E-Health systems and defines the set of challenges and research gap across the IoT-based E-Health systems.

Further research into challenges faced by IoT and the key technologies involved can be observed in [8]. Some of the technologies discussed in details are identification technology, IoT architecture technology, communication technology, network technology, network discovery technology, software's and algorithms, hardware technology, data and signal processing technology, discovery and search engine technology, relationship network management technology, power and energy storage technology, security and privacy technologies, and standardization. Various perspectives and applications of the IoT systems have been discussed in detail within this paper. It provides a

complete description to significant technological drivers, potential applications, challenges and research gaps in IoT. The entire state of art of Iot has been discussed in brief in this paper.

The importance of authentication can be understood in [9], where the property of security across E-healthcare clouds is preserved through the process of three factor mutual authentication scheme. It uses a combination of the smart card, password, and user biometric identity to perform the three-factor mutual authentication process. This helps to provide additional security to protect data and such mechanism also helps to improve data security strength in healthcare systems. Also, it adds the property of user revocation to the mobile devices. This is useful in case the users would be revoked when the mobile device is stolen. Thus this also helps to provide security across E-Health mobile computing environment.

In context of mobile security which is an important aspect of E-health, cryptography based protocols are one of the many techniques that help provide authentication, identification and privacy protection. It uses an ad hoc protocol when a mobile node joins a new cluster. Such protocol uses request-reply authentication messages and can be an effective method to protect against eavesdropping, tracking location of devices etc. Beside this, other techniques used involve RFID (Radio Frequency Identification) systems based on EPC network environment which automatically identifies tagged objects by using RF signals. A brief description of the security and privacy issues across mobile telecare and cloud-assisted E-Health systems are given in [10]. It also uses hybrid cryptographic access control methods for cloud based healthcare systems. The cryptographic method has been used to establish session keys which help to communicate information using the Kerberos protocol. Location based and biometric based authentication methods are used to authorize users. The doctors monitor patient's health conditions from the remote areas through telecare applications. This framework helps to monitor and analyze patient's health in a secure and efficient manner and is also capable of handling HER's in a secure and well ordered manner.

The application of cloud paradigm in E-Healthcare systems is given in [11]. It explains in brief the advantages of using cloud computing in biomedicine. As we have discussed before, in real time health monitoring, the amount of data accumulated from various patients is so large that it cannot be stored by using traditional means. Cloud computing storage services plays a major role in the research of biomedicine technologies. A secure cloud architecture for Iot and healthcare systems is given in [12]. It points out the security issues in both cloud computing and mobile telecare. It proposes an efficient model that allows doctors to remotely monitor their patient through mobile application by using the cloud. It combines smartphone, bluetooth and cloud to share patient data in a secure and confidential manner. The model also provides the ability to handle large data sizes and effective user revocation. An innovative architecture for E-health systems has been introduced in this work, such that the data collected from the sensor networks are easily processed and managed across the cloud computing environment. It simplifies the process of data sharing by solving the drawbacks of the existing E-Health systems. Also this architecture provides a flexible and effective CP-ABE based access control algorithm for E-Health clouds. Further, it deals with patients emergency situations in an efficient manner.

The next section states the proposed model of this paper.

III. PROPOSED ARCHITECTURE

In this paper, a model has been proposed that takes into consideration the various aspects of a healthcare system that we have discussed above. As we know IoT makes use of sensors to collect data about the patient's health condition. These are small sensor nodes that help to measure physical conditions like pulse rate, body temperature, respiratory rate etc to name a few. Some of the recommended sensors that could be implemented are blood pressure and blood oxygen level measuring sensors as they help to determine the vitals of a patient. There can also be special purpose sensors like blood glucose, sugar level, special joint angle sensors. If these could be implemented properly, then they can be used to treat special conditions. Sometimes one of these sensor nodes act as a central node that acts as a device for data collection and processing hub. It might also be capable of decision making and might send some information to an external location. Today smartphones are the preferred choice of central hub as they are easy to use and offer an advanced processing as well as communication capability at an affordable price. Such smartphones can also be customized as per need and use of healthcare. These sensors are necessary as they help personnel to monitor their patients in real time environment, analyze their health conditions and provide feedback depending on their analysis from distant facilities. This is where IoT gives both patients and healthcare personnel major advantage as one can get feedback on their health issues by simply staying in the comfort of their home and not visiting some expensive healthcare facility every day. Depending on the condition of the patient and the type of sensors required, this proposed model can be used for remote health monitoring for a wide variety of health issues. In the figure, all the sensors send the information to a node called decision making node whose function is explained in the later part.

Generally, the wearable sensor nodes need to communicate with the central node. For this, a short range communication needs to be established. In general, wireless external wearable nodes are preferred as compared to implanted sensors or vision based sensors. As a result the communication method should be chosen in such a way that it has no negative effect on a human body because patients do not want any additional health concerns. So the communication process is chosen in a way that it takes care of certain things like how it affects the human body, security of data and latency. It needs to ensure strong security mechanism is provided for protecting sensitive information regarding the health conditions of patients, so that it cannot be accessed by any attacker or unauthorized third party. Also in such systems it has been observed that time delays play a major role like calling an ambulance when an emergency situation arises. Low latency is required for such time critical situations. Sometimes a time delay of a few minutes can result in the life or death of a patient. Thus, high priority should be given to low latency, maximum possible security and on the effects of the communication standard on the human body. The proposed model uses LPWAN(Low Power Wide Area Networks). The range of a LPWAN is generally several kilometers, even in an urban environment which is much more than the range of Wi-fi or bluetooth. This is worth using for a large number of healthcare applications that includes monitoring general health and receiving hourly updates,

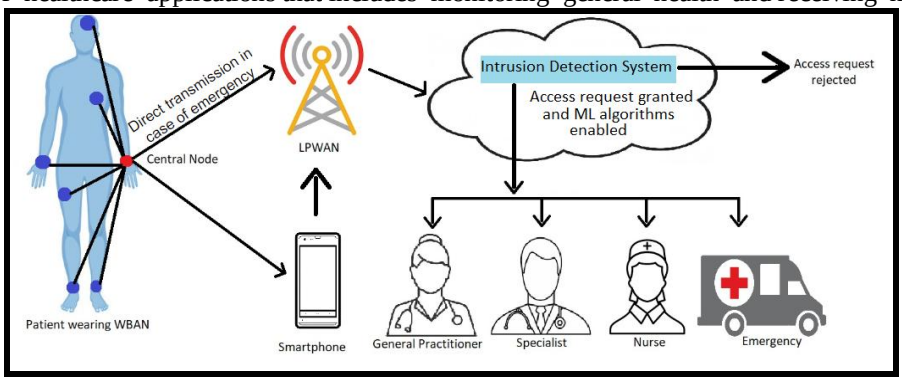

Fig.1. Proposed Architecture

monitoring critical health and receiving emergency calls, and rehabilitation where updates may only be necessary once daily. As Fig.1 depicts, all the data from the remote sensors has been sent to the decision making node that can be viewed through the smartphone and then uploaded on the cloud through the getaway. However there might be situations when the patient might not be healthy enough or is in dire need of immediate medical assistance, only if such conditions arises, then the decision making node has the ability to directly communicate with the cloud and inform the respective healthcare practitioner of the patient's current situation. Under normal condition, it sends all the data to the smartphone.

For storing the patient's personal information, here a general cloud storage architecture has been used. In a cloud based architecture, there is a trusted cloud service provider who provides cloud storage facility to store a patient's healthcare information. The service provider can make use of public, private or hybrid cloud infrastructures to store information about a patient's physiological conditions that are monitored with the help of the wearable sensors. The body sensors project the information to the cloud servers for storage purposes. The patients can also track their health related information with the help of their mobile devices. Medical information obtained from different patients need to be stored. The reason behind using cloud is that the data stored in cloud, not only helps in the treatment of the current patient but can also be used as case studies to help find solutions to other patient's illness. Doctors benefit from studying these medical history available in the cloud database. Based on the literature study in this paper, it is evident that cloud storage is one of the most viable methods for storing data but the size of the database used to store data in cloud needs to be very large to efficiently apply machine learning. Machine learning algorithms can be implemented to help track a patient's progress, what parameters is making their conditions worse, predict how long they will take to be fully rehabilitated etc. This kind of algorithms can be modified depending on what type of wearables are used and what kind of information can be stored by using them. Many researchers have even suggested some highly optimized machine learning algorithms that can help predict situations when the patient's blood pressure will be highest by using a comprehensive record of the patient's blood pressure data. This information can help determine optimal times for the patient to take any medication that they may require to manage their condition, and remind the patient of using a buzzer or alarm on the central node.

To make the proposed model secure, the Intrusion detection system has been introduced in the cloud. This deals with authentication and authorization of the individuals involved in the system. The Intrusion detection system helps to detect malicious activity and policy violations. The use of this system for detecting intrusions on computer

systems can be considered as a way to build an efficient and adaptive healthcare system. When data access is requested in the cloud by a particular patient healthcare personnel involved with the patient, there is a need to identify and separate them from unauthorized users. So the main objective is to detect these anomalies and catch the hackers before they can do real damage to the network or misuse the patient's healthcare record. Now these hackers can be network or host based. A network-based intrusion detection system resides on the network, as can be seen in the figure. The Intrusion detection system generally works by either looking for signatures of known attacks that have happened earlier or deviations from the normal day to day activity. These deviations or anomalies are pushed up the stack and examined at the protocol and application layer. If an anomaly is detected, then the system will reject the request for data access. However, if no anomaly is detected, then the access to the user's data will be granted. Finally, machine learning algorithms are implemented to perform diagnostics or provide treatment plans. This makes it easier for doctors to read the patient's data, to help in data management etc and the most important use is to detect abnormalities in the patient's physiological data. This is an extremely valuable utility with respect to healthcare context. An example has already been discussed about using machine learning algorithm on ECG signals that helped detect congestive heart failure. Similarly, the algorithms can also be applied on EEG, ECS, data recorded from motion sensors to help identify deviation in the physiological data collected from the WBANs. And in case, some abnormal deviation is suddenly detected, it can help alert the nearby healthcare centres to provide the necessary aid.
The next section concludes the paper.

IV. CONCLUSION

Thus it can be observed that IoT has a huge impact in the world of healthcare and will continue to advance in the near future. This survey paper involved a literature study of various healthcare system models using machine learning and cloud computing, the overview of types of security issues faced in E-Healthcare systems and a proposed model involving WBANs, machine learning algorithms, cloud technologies, Intrusion Detection system. The future scope of the proposed model is very wide since the paper proposes a model for future IoT-based healthcare systems, which is applicable to both general systems and systems that monitor specific conditions. This makes the model both flexible and highly efficient. Keeping security in mind, an Intrusion detection system has been included to strengthen security of the system. This system is easily available and the users can even implement their own set of rules in some systems. In the future, further developments can be done to make the model more robust and cost effective.

V. REFERENCE

[1] Prosanta Gope, T.Hwang, "BSN-Care: A Secure IoT-Based Modern Healthcare System Using Body Sensor Network", IEEE Sensors Journal, vol 16, Issue 5, March 2016.
[2] S. Ghanavati, J. Abawajy, and D. Izadi, "An alternative sensor Cloud architecture for vital signs monitoring," 2016 International Joint Conference on Neural Networks (IJCNN), pp. 2827–2833, 2016.
[3] K. Lin, F. Xia, W. Wang, D. Tian, and J. Song, "System Design for Big Data Application in Emotion-Aware Healthcare," IEEE Access, vol. 4, pp. 6901–6909, 2016.
[4] P. K. Sahoo, S. K. Mohapatra, and S. L. Wu, "Analyzing Healthcare Big Data With Prediction for Future Health Condition," IEEE Access, vol. 4, pp. 9786–9799, 2016.
[5] C. Y. Hung, W. C. Chen, P. T. Lai, C. H. Lin, and C. C. Lee, "Comparing deep neural network and other machine learning algorithms for stroke prediction in a large-scale population-based electronic medical claims database," 2017 39th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), pp. 3110–3113, 2017.
[6] J. Park, K. Y. Kim, and O. Kwon, "Comparison of machine learning algorithms to predict psychological wellness indices for ubiquitous healthcare system design," Proceedings of the 2014 International Conference on Innovative Design and Manufacturing (ICIDM), pp. 263–269, 2014.
[7] Islam, SM Riazul, et al. "The internet of things for health care: a comprehensive survey." IEEE Access 3 (2015): 678-708.
[8] Debasis Bandyopadhyay and Jaydip Sen. "Internet of things: Applications and challenges in technology and standardization." Wireless Personal Communications 58.1 (2011): 49-69.
[9] Jiang, Qi, et al. "A privacy preserving three-factor authentication protocol for e-Health clouds." The Journal of Supercomputing 72.10 (2016): 3826-3849.
[10] Premarathne, Uthpala, et al. "Hybrid cryptographic access control for cloud-based EHR systems." IEEE Cloud Computing 3.4 (2016): 58-64.
[11] Sobeslav, Vladimir, et al. "Use of cloud computing in biomedicine." Journal of Biomolecular Structure and Dynamics 34.12 (2016): 2688-2697.
[12] Thilakanathan, Danan, et al. "A platform for secure monitoring and sharing of generic health data in the Cloud." Future Generation Computer Systems 35 (2014): 102-113.