IoT on E-Health: Application and Security Challenges

Soumen Halder and Anubrata Das

Department of Computer Science, Ramakrishna Mission Vivekananda Centenary College, Rahara, Kolkata, India

*Corresponding author: soumen100@rkmvccrahara.org \ dasanubrata833@gmail.com

ABSTRACT

IoT is short for Internet of things. The main objective of IoT is to refer the network of physical object that obtains a IP Address for internet connectivity. The expansion of has great effect on medical, education, transportation, agriculture etc. The cost estimation in medical perspective has been lessen upto a great amount by introducing the IoT in medical. E-health applications has led to increase the concerns of security and privacy, especially in healthcare domain. In fact, healthcare applications are prone to data breaches. In security aspects in medical the E-health applications are use widely by using the internet of things. 

Keywords: IoT, Security services. E-health, Security Challenges, Adaptive Security

E-health is becoming an emerging field these days in every perspective. Medical, business related all information are delivered and enhanced by internet. In the medical field IoT has opened a new scenario. Symptoms and tends are insights very well to detect a particular disease. It has helped a lot in the view of E-health.

CYRORE is a smart monitoring system which helps to less severe symptoms to detect cancer and its treatment. It doesn’t need any patient the weekly visit.

A Continuous Glucose Monitor (CGM) is a device that helps diabetics to continuously monitor their blood glucose levels for several days at a time, by taking readings at regular intervals. The first CGM system was approved by the US Food and Drug Administration (FDA) in 1999, and in recent years, a number of smart CGMs have hit the market.

As more of these devices are brought to market and even become available as prescription medication, for example on the NHS, digital healthcare will start to become the rule rather than the exception. With the availability of such devices the medical field is opened to all now a days very widely. For example on the NHS, digital healthcare will start to become the rule rather than the exception.
LITERATURE REVIEW

The author in[1] describes that in the improvement of E-health many benefits has been provided by the emerging IoT. In this case on of the most important thing is ensuring the security and privacy about the processing capability and resource use. The chance of attack is very less as most communications are wireless. Most IoT components are constrained by energy, communication and computation capabilities which is necessary for the implementation of complex security supportive schemes. They basically focused on a risk based adaptive security framework for IoTs in E-health that will predict risk damages. The paper also elaborates that IoTs benefits in Game theory and context awareness technique and validation case study.

The author in[2] has developed Wireless Body Area Network that sent vital sigs of a patient using low rate communication media. Their main focus is to improve the E health application that is an important part of IoT. This project requires an environment with adaptive security solutions in realistic simulations. The paper actually describes the setup of a testbed for adaptive security for IoT using current commercial off-the-shelf software and open source software. It also discussed about the validation of the setup through discussing the impact on antenna orientation on energy consumption. This will particularly be successful when studying the feasibility of the adaptive lightweight security solutions will be the part of ASSET(Adaptive Security for Smart Internet of Things in E-health) project.

The author in[3] describes that the successful deployment of IoT based E-health rely on overcome the major security concerns for the users those needs to be addressed in the energy efficient way. The security will be mainly provided against Impersonation attack, man in the middle attack, and unknown key sharing attacks for IoT based E-health domain. The research proposed a secure group based lightweight authentication and energy efficient and computation for health care to IoT based applications. Which will use elliptic curve cryptography(ECG) principals that provide mentioned featured of suggested model.

This author in paper[4] integrates run-time verification enablers in the feedback adaptation loop of the ASSET in the e-Health settings and instantiates the resulting framework with Colored Petri Nets. The run-time enablers make machine-readable formal models of a system state and context available at runtime. Therefore, the integration of run-time enablers into the ASSET adaptive framework could lead to a sustainable security framework for IoT in e-Health.

The author in paper[5] describes Internet of Things (IoT) offers a seamless platform to connect people and objects to one another for enriching and making our lives easier. This paper discusses about applicability of IoT in healthcare and medicine by presenting a holistic architecture of IoT e-Health ecosystem, rising aging population with chronic diseases:

- Device
- Fog computing and
- Cloud to empower handling of complex data in terms of its variety, speed, and latency.

E-medicine, implants, early warning systems, to population monitoring in smart cities. Then they finally address the challenges of IoT e-Health such as data management, scalability, regulations.

This subsection mentions studies which proposed and implemented different lightweight algorithms or schemes for securing IoT systems.
Objective

In this paper basically focuses on successful deployment of IoT based E-health rely on overcome the major security concerns for the users those needs to be addressed in the energy efficient way. An assessment framework to evaluate adaptive security algorithms specifically for the Internet of Things (IoT) in e-Health applications has been presented here. We also focused on the applicability of IoT in healthcare and medicine by presenting a holistic architecture of IoT e-Health ecosystem, rising aging population with chronic diseases. And last but not the last the paper has gone through how IoT is applicable in the field of E-Health and some advance use of it.

APPLICATION OF IOT ON E-HEALTH

IoT has a signification contribution in healthcare industry. IoT applications in healthcare that benefit patients, families, doctors and hospitals. Remote monitoring system using enabled devices converted healthcare system easier and faster. It expected that IoT health care market will be 163 billion by end of year 2020.

- Using different wireless equipment embedded with IoT help monitoring patients’ health. Doctors can keep track patients’ health condition, and if any emergency occur immediately doctor can address the patients. Even needs of Oxygen and other medical specifications.

- U.S Breast Cancer Statistics shows that about every 1 woman over 8 women nearly almost 12% effected by Breast cancer\(^{[10]}\). In 2020, estimated 276,480 new cases may increase. 2.1 million women effected by breast cancer in each year\(^{[9]}\). This numbers just describe that ‘treat of Breast cancer’. To prevent this IoT can lead a great roll. By measuring breast temperature of breast in very frequently and then using Data analysis one simple prediction can help a lot. Even this kind of warning can help women to take required steps.
Fig 2: Incident of Breast cancer of U.S

- Wireless IoT devices help monitoring blood pressure, glucose monitoring, heart rate etc. For instance, if a blood pressure reading of patient is 140 mmHg then IoT devices send feedback to the patient[7].

Fig. 3: ECG-Sensor with Arduino configuration
AI-IoT based different technologies can help save many lives against cancer by early-warning systems. And the marriage of AI and IoT can help enormously in cancer cure and Medical diagnosis.

IoT devices help to collect data and that can use in future research. Using data analytic tools and Image processing many deceases can identify or the state of the decease, required medicine can be discovered.

ADVANCE USE OF IoT

In section-3 we mention some effective application of IoT, basic it follows one general algorithm for e-health application. First IoT sensors those are use together arduino board collect data from human, then using Internet it send data to a dedicated mobile application. And then display result based on algorithm. Data flow model describe it clearly -

Often doctors are not available for each patient all time of the day, but many time patients are required one doctor. To overcome such situation IoT based mobile application can help a lot. Doctor can observe required measures through smart IoT based application and can send his suggestions.
We propose one general frame-work for mobile health;

1. Input: pin
2. OutPut: Smart suggestion

(a) step 1: Read row data from patient body using IoT sensor
(b) step 2: Arduino bord complete connection with sensors
(c) step 3: wi-fi module like NodeMcu ESP8266 send data through Internet
(d) step 4: Doctor can see frequent results and improvement of patient through Mobile
(e) step 5: Doctor send suggestion Using smart AI tools
(f) step 6: Madical sport team even patient also can take necessary steps according to the suggestion

Fig. 6: Different sensors use in human body for health Monitoring

MORE APPLICATION OF IoT

IoT has several uses, Starting from agriculture to space science. IoT used in different domain like education, Metro station, Air-port, shopping mail, Hospitals, security[8]. some example application are only explain in this research.
In smart cities IoT sensor use found free parking space. IoT sensor use to found cars among large number of cars.

Unexpected events like accidents or traffic update in roads can be observed from remote place. It helps define velocity of cars in highways.

In domestic uses IoT based light, fan, Ac, water purifier is very helpful in ongoing days. It help to save lot energy and that passively help to save money. Remote control switches help save human effort and energy.

IoT based smart system help in oxygen bars for controlling oxygen level remotely.

Using AQI sensors prediction and observation of atmosphere become truly easy.

CONCLUSION

In the research we try to explain important of IoT in Health-sector and when we use an electronic device for transport data or use the data in that very point question of security arise question of security. we manly try to describe some security modulus. From among modules group-based lightweight authentication scheme is good it can prevent different kinds hacking. But in the question of security we need some more power-full algorithm as some this scheme is not working properly in long distance. In future we are try to make some algorithms for security modules.

REFERENCES


