RELIABLE AND SECURE HEALTH IOT FOR PATIENT MONITORING WITH BIO-SENSORS IN CLOUD COMPUTING

Sonam V Maju

Student, Department of Computer Science and Engineering, KMEA Engineering College, Ernakulam, India,
Email:Sonammaju22@gmail.com

Abeera V.P

Assistant Professor, Department of Computer Science and Engineering, KMEA Engineering College, Ernakulam, India

ABSTRACT: As global ageing and chronic diseases are increasing day by day,we need a revolution from hospital centric to home centric. The idea proposed here is an application of Health IoT,where continuous monitoring of old aged people is done through bio-sensors and non-compliance problem is controlled through a medicine box which gives alerts through light and sound indicators as medical reminders.The technical era is opting a heart authentication mechanism and so heart beat signals of a patient have to be secured as well.A reliable and secured mechanism is developed here for the secured heartbeat authentication in the cloud environment.A new cryptographic method is developed for security in the cloudsim architecture.

Keywords:Bio-sensors,Health IoT,Medicine Box,Cloud sim,Cryptography in cloud

I.INTRODUCTION

By largely using and promoting Home Health IoT the facilities and services of hospitals can be made available in our home atmosphere itself. IoT ensures a technical world of devices and things newly outfitted with Internet, that will be able to continuously monitor, interact, communicate and react with the environment change. All that new information is going to need to be collected and studied, a thread that can effortlessly surpass IT's own in-house server capacity. So it is that the cloud, as one coder/developer put it, it will be the surreptitious warhead in the Internet of Things. That's because the cloud functions as the corresponding to a big data centre contributing the system scale that will allow IT to host, store and process the huge increase in the quantity of data occupied by IoT.

IT administrators take hands-on measures to connect IoT with cloud deployments, they need to consider security vulnerabilities, which always accompany technology revolutions. The level of IoT ensures a promising future with more implementations of hardware for gathering information from cameras and bio-sensors. This work is trying to ensure the adequate provisioning of user authentication, encryption/decryption and integrity of protections through the IoT infrastructure in order to guarantee both the privacy and the integration of data being collected.

Currently chronic diseases and number of patients are being a common concern. So hospital restructuring and thereby encouraging home healthcare is very important. Home healthcare services can be efficiently made practical with the

promising technology of Internet-of- Things.An intelligent home-based IoT Platform is proposed here, where the Home Health-IoT, is explored, studied and deployed. In particular, the Home Health-IoT involves bio-sensors for reading the human heart rate in digital format ,an intelligent medicine box (iMedBox) with enhanced connectivity and interchange ability for the integration of devices and it is connected with a light sensor to read the variations in the medicine slots like counting the number of tablets a patient is consuming. Thus this home health IoT platform can continuously monitor the patient and can provide proper alarms and trigger a message when there is any abnormal variation in the pulse rate. Alert messages can be given if the patient is taking wrong medicines and can set a reminder as well. The sensor readings and the contact details of emergency centers can be stored in the servers.The status of the patient is generated every day and is stored in the server in the encrypted format. The encryption algorithm used here is the arithmetic part of elliptial curve cryptography without generating a curve. This platform flawlessly fuse IoT devices with in-home healthcare services for an improved user experience and service efficiency.

II. LITERATURE SURVEY

Alok Kulkarni, Sampada Sathe's [2] paper about healthcare internet applications, discuss about the evolution of internet, its concise discussion and applications. IoT is a physical network of objects or smart things preset with electronics, related software, bio-sensors and connectivity to permit it to achieve higher values and facilities by exchanging data with the firm operators and other connected devices.

David Niewolny in his paper describes, 'How the Internet of Things Is Revolutionizing Healthcare' [3] is discussing about the reasons for emergence of IoT and designs of applications where IoT is used. The issue is people have only limited time, awareness and accuracy, which means they won't be able to capture data about things networked in the real world consistently.

Different sensors are accessible and available in the market for providing ad ensuring home healthcare, S. Tozlu, M. Senel, W. Mao, and A. Keshavarzian in his paper[4] Wi-Fi enabled sensors for internet of things describes a practical approach, and give explanations about different sensors available.

Mario Ballano Barcena Candid Wuees in the study report, Insecurity in the Internet of Things[9], and Ignacio M. Llorente,Head of DSA-Research Group[10] explains the integration of cloud services and IoT. IoT ensures large quantities of new devices that will be deployed or rooted right through an organization. Data captured from these devices can then be analyzed and acted upon. In few cases, the devices are proficient of performing some tasks. These described edge devices will allow for huge data gathering activities. The analysis of this data will allow beforehand hidden linkages to be made which may reason anxiety for the privacy of individuals or groups of people. In few cases, individuals may not even be bothered of being tracked or recorded giving the ability for next generation microchips to be entrenched in practically any platform. In all cases, assuring the security of each component within an IoT system is important to keep malicious users from intriguing advantage of the power of the IoT in an unauthorized manner.

III.BACKGROUND

A promising trend in healthcare is to shift routine medical checks and other healthcare services from hospital (Hospital-Centric) to the home environment (Home-Centric). By doing so, first, the patients can get seamless healthcare at anytime in a comfortable home environment; next, society's financial load could be greatly reduced by remote treatment; third, partial hospital resources are made available only for people in call for of emergency care. In-home healthcare and services can drastically reduce the total spending on medical care or treatment.

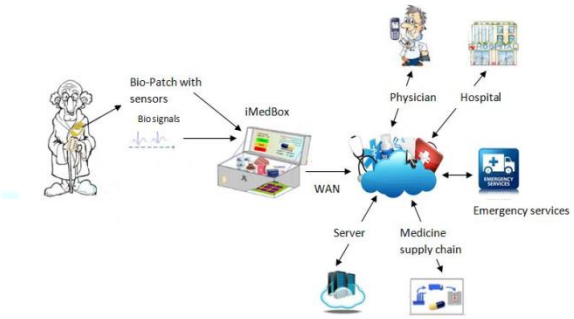

Fig 1: Home Healthcare System in Cloud

Cloud computing acts as a front end to access Internet of Things and is more popular service that comes with more characteristics and advantages. The cloud computing and Internet of things are tightly coupled in the this will lead to the production of large amounts of data, further the need to be store these data, process and access. Cloud computing as a paradigm for big data storage and analytics. The real and exciting innovation will come from combining IoT with cloud computing. The blending of cloud computing and IoT can enable sensing services and influential processing of sensing data stream. Denial of service is the greatest security threat to cloud computing. Malicious insiders, which can be their employee or a business partner who have access to a network, system, or data for malicious and unauthorised purposes. In an inappropriately designed cloud set-up, a malicious insider can wreak even greater havoc. Top security intimidation to cloud computing is insufficient due to meticulousness; that is, organizations hold close the cloud without fully understanding the cloud environment and associated risks. Cloud abuse, ie.using a cloud service to break an encryption key is too difficult to break on a standard computer. So in order to protect the data which is stored in the cloud environment, in this project a new and simple method is used for securing the authentication process for the cloud owners. Implementing Cloud is the next stage, as we couldn‟t create a cloud as such, we are simulating a cloud environment which shows all the data stored by each user, its reports and analytics. The simulation tool that we are using here is the cloud sim which gives the datacenter, broker details and processing time of each execution. Cloud Sim is a toolkit for modelling and simulating cloud environments and to gauge reserve provisioning algorithms. It provides a generalised and extendable simulation model that ensures flawless modelling and simulation of application performance. By means of CloudSim, developers can focus on specific systems design issues that they want to inspect, without getting troubled about details related to cloud-based infrastructures and services. Cloud Sim is the simulation engine that provides an user friendly interface, report generation features and design of extensions in a plug-in fashion.

The CloudSim layer provides hold for modelling and simulation of cloud environments together with committed administration interfaces for memory, storage, bandwidth and VMs. It also necessities hosts to VMs, application implementation management and energetic system state monitoring. A cloud service provider can employ customised strategies at this level to study the effectiveness of

different policies in Virtual machines provisioning. The user code layer exposes basic entities such as the number of machines, specifications, etc, as well as applications, Virtual machines, number of users, application types and scheduling policies.

In this project authentication is done in cloud sim in the following manner. Each user/patient heartbeat details will be collected and monitored using the health IoT architecture and the data collected in these manner require large storage area like cloud environment. As the security threats faced by the cloud environment is very large and still the software engineers and techies are trying with all the emerging technologies to solve the security issues. I am proposing an idea in this project and thereby securing the authentication of each user to the cloud storage. When each user saves or copies a particular file to the cloud storage, an encryption method is generated using the name of file, length of the file and a password, all these three entries will be converted to the binary format and concatenated. This concatenated binary value is stored in the database. Inorder to open the stored file, again the name of the file, length and password is converted to binary and concatenated, then this newly generated binary value is compared with the stored values in the database. If the stored and generated value matches with each other, then only the stored file will be opened automatically. This is the security mechanism proposed in this project to solve the security problems of the cloud.

IV.IMPLEMENTATION

An IoT application in the health platform which involves heartbeat sensors for reading the human heart rate in digital format which will be further encrypted and stored. An intelligent medicine box with a green light sensor to give medication reminders and red light sensor to indicate the variations in the medicine slots like counting the number of tablets a patient is consuming, alarms are there for consuming wrong medicine.

In order to protect the files stored in the cloud environment, an encryption method is proposed while saving a file to the cloud, the encryption is done by taking the features and properties of the file not with the file content. The encrypted value thus obtained in the binary form is stored in the database. If the user want to open a file stored in the cloud environment, the decryption is done with the file properties and the binary value thus obtained is compared with the stored binary value. If both the values matches, then the file will be automatically opened.

Encryption Method:

- After the user entered into the cloud environment, he/she needs to browse the file to be stored.
- The filename,length,cloud capacity and password have to be inserted and press the encryption button.
- All the entered value except the password is converted to binary format.
- The password is first converted to ASCII format and then to the corresponding binary format.
- All these binary values are concatenated and will get a lengthy binary value which is stored in the database.

Decryption Method:

- In order to open the stored file,the user need to give the file name,cloud storage value and the password.
- The concatenated binary value will be generated and is compared with the stored value in the database.

- If both the values match with each other,the selected file will be opened automatically.
- Otherwise, a mismatch will occur and an access denied message will appear.

V.CONCLUSION AND FUTURE SCOPE

An IoT-based intelligent home-centric healthcare IOT platform, which flawlessly connects smart sensors attached to human body for biological monitoring and intelligent medical packaging for daily medication management. Heartbeat authentication is the authentoication mechanism used in the next era.

NymiBand,AT&T,EMC,Halifax,ElectronicFrontier Foundation are some of the fields and products which uses heartbeat authentication. So the heartbeat readings stored in cloud have to be protected and only authorized users should be able to access the heartbeat readings. The proposed encryption mechanism can guarantee cloud security to a certain limit. Today, the most widely adapted technology for the Internet is the standard web services. Wireless identifiable embedded healthcare systems at the edge of the network should be connected to web services and make use of comparable functionalities and this will prove to be a challenge in the future for the internet especially in the cloud environment.Cloud Security is one main reason that is been faced by the developers and in future the next reason will be the shortage of space as the big data will be merged with the IoT as well as cloud platform.These millions of components produce, analyse, consume and process information in dissimilar healthcare environments such as hospitals, households and nursing homes as well as in the work and everyday lives of people. The Internet of Things will change our society, and will bring seamless 'anytime, anywhere' personalized healthcare and monitoring over fast reliable and secure networks. This implies that we are approaching the end of the divide present between digital, virtual and physical worlds.

REFERENCES

[1] Geng Yang, Li Xie, *"A Health-IoT Platform Based on theIntegration of Intelligent Packaging, Unobtrusive Bio-Sensor, and Intelligent Medicine Box",* IEEE transactions on industrial informatics, vol. 10, no. 4, november 2014, Matti Mäntysalo, Xiaolin Zhou, Member, IEEE, Zhibo Pang, Li Da Xu, Senior Member, IEEE,Sharon Kao-Walter, Qiang Chen, and Li-Rong Zheng, Senior Member, IEEE

[2] Alok Kulkarni, Sampada Sathe "*Healthcare applications of the Internet of Things:A Review*" ,*Department of Electronics and Telecommunication, Computer Engineering Pune University, Maharashtra, India*, Alok Kulkar et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (5) , 2014, 6229-6232

[3] David Niewolny,"*How the Internet of Things Is Revolutionizing Healthcare*",Healthcare Segment Manager, Freescale Semiconductor

[4] S. Tozlu, M. Senel, W. Mao, and A. Keshavarzian, *"Wi-Fi enabled sensors for internet of things: A practical approach,"* IEEE Commun. Mag., vol. 50, no. 6, pp. 134–143, Jun. 2012.

[5] Elaine Brow "*Elliptic Curve Cryptography"* , December 2010 Math 189A: Algebraic Geometry.

[6] C. E. Koop et al., "*Future delivery of health care: Cybercare,"* IEEE Eng. Med. Biol. Mag., vol. 27, no. 6, pp. 29–38, Nov. 2008.

[7] Z. Pang, "*Technologies and architectures of the Internet-of-Things (IoT) for health and well-being,"* Ph.D. dissertation, Dept. Electron. Syst., School Inf. Commun. Technol., Royal Inst. Technology (KTH), Stockholm, Sweden, 2013.

[8] Aakash Sunil Salgia*, K. Ganesan and Ashwin Raghunath, "*Smart Pill Box", Indian Journal of Science and Technology, Vol 8(S2), 189–194, January 2015.*

[9]Nabil GHANMY, Lamia CHAARI FOURATI, Lotfi KAMOUN *"Elliptic curve cryptography for WSN and SPA attacks method for energy evaluation*", Electronic and Information Technology Lab (LETI), ENIS SFAX University, Tunisia