Cloud Integration of E-Health Wireless Sensor Networks for Data Privacy

Dr. AMIT VERMA[1], MADHU[2], AMANDEEP KAUR[3]
[1]*Professor and Head of Department, Department of computer Science, CEC Landran, Mohali, Punjab*
[2]*Mtech Research Scholar, Department of computer Science, CEC Landran, Mohali, Punjab*
[3]*Assitant Professor, Department of computer Science, CEC Landran, Mohali, Punjab*

Abstract- Information security and privacy is an issue of importance in healthcare area. The adoption of digital patient's record, increased regulation, provider consolidation and the increased need for information exchange between the patients and doctors need the better information security. We will survey on the need of information security and privacy in the healthcare system. As Healthcare is always an important issue, as it presents the better class of life the personalities can have. Individual monitoring is required on a periodic check basis as, it is always better to avert an infirmity than to treat it.

Keywords- bio medical application, wireless sensor network, mobile, healthcare monitoring, deployment

I. INTRODUCTION

Healthcare is always an important issue, as it presents the better class of life the personalities can have. Individual monitoring is required on a periodic check basis as, it is always better to avert an infirmity than to treat it. The growing age populace of the countries presents a mounting piece of government's funds and has new confronts to health care schemes, mainly with old age people who are staying on sovereign senior housing. Traditionally, the healthcare checking was executed on a periodic basis, where the tolerant have to keep in mind its signs of the disease; and the doctor executes several checks and prepares a analytical report, then examines patient improvement along the treatment, if feasible. The medicinal uses are of two types: Implanted and Wearable. The wearable applications are employed on the body of an individual or at closeness of the client. And the Implantable devices are those which are introduced within human body. Several other applications are also there e.g. location of the person and body position measurement, generally examining of people who are not well in hospitals and at their residence. Wireless body area networks can collect data about an individual's energy expenditure, health and wellness. In this thesis the main focus is on healthcare applications and ECG of patients is monitored.

A. Characteristics of wireless sensor networks in healthcare

The wireless sensor network is utilized for real world un-attended substantial surroundings to compute several constraints. There are number of characteristics of WSN that should be believed for proficient use of the network. The important characteristics of WSN are given below:

Low cost: In the sensor networks usually hundreds, thousands or even any number of wireless nodes are organized to compute any physical surroundings. Sequentially to lessen the entire charge of the network area the price of the wireless sensor node ought to be set aside as low as probable.

Computational power: In general the sensor nodes have restricted computational abilities as the cost and energy have to be considered.

Energy efficient: In this the WSN is utilized for diverse purposes like computation, storage and communication. Sensor motes devour more energy as compared to any other for communiqué. If sensor nodes run out of the power they can habitually befall unfounded as we do not have any alternative to recharge. Accordingly the protocols and algorithms growth ought to consider the power utilization in the devise phase.

Communication Capabilities: The WSN usually communicates using radio waves in the wireless sensor channel. This has the characteristic of communicating with squat range, using slight and dynamic bandwidth. And communiqué channel can either be bi-directional or uni-directional. With an not attended and unfriendly operational environment it is complicated to run WSN efficiently. Therefore, the hardware and software for communiqué should judge the robustness, security and resiliency.

Dynamic network topology: The common WSN are also known as dynamic network. Sensor node can fall short with battery collapse or with other situations and communiqué channel can be disturbed plus the further sensor node may be supplementary to the wireless area that outcome the instant alterations in the topology of the network. Therefore, the sensor node should further with the purpose of re-configuration and self-adjustment.

B. Cloud Integration of Healthcare Monitoring

Wireless sensor network characteristically consist of a compilation of sensors with their own energy involvement, data storage, data processing capability and wireless communication. In a distinctive wireless network, every mote has a micro processor with partial dispensation capability, the miniature amount of reminiscence for signal dispensation and has restricted energy provide and bandwidth. Every sensor node communes through wireless network with only some narrow nodes within its radio communiqué assortment. The data gathered by and broadcasted on a wireless sensor network explains circumstances of substantial surroundings like humidity, temperature, or quivering. Uses of wireless networks are used in spacious range and can diverge considerably in useful desires. Some sample applications include: Natural disaster prevention, Traffic examining, Forest fire detection, Habitat monitoring, Healthcare examination etc. Non contact electro-cardiogram (ECG) method has been gaining fame now a day because of its non invasive convenience and features in every daily life use. Cloud computing in mobile has been presented for a health scheme where a non contact ECG scheme is used to confine medical signals from clients. The healthcare service is offered to gather medical signals from several locations on periodic check basis. To examine and evaluate the ECG signals in synchronized way, the mobile device is utilized as a mo bile examining terminal. Besides this, an adapted healthcare subordinate is also mounted on the mobile tool; many healthcare attributes such as drug QR code scanning, health status summaries, and prompts are incorporated into the applications of mobile. Data of health are being coordinated into the healthcare compute service i.e (web server data set and web server system) to make sure a faultless healthcare examining system and anywhere and anytime reporting of network association is accessible.

C. Requirement of Cryptography Key Exchange in Cloud Based Wireless Sensor Network for Health-care Monitoring

The wireless Sensor area is a set of sensor nodes which builds up a network by radio communication in an independent and distributed way. These nodes are dispersed over a definite field, and are able to gather and relay information about the surroundings, in order to offer fine grained observations of a fact. The sensor nodes are generally, prepared with one or more sensors which are used for capturing events from the environment, an analog-digital converter, a central processing unit, a radio transceiver with imperfect computational capabilities, a small quantity of memory and the battery. Sensor devices combine with one another in order to perform basic operations such as communication, sensing and processing of data. Main applications using wireless networks include: environment checking, healthcare, entertainment, animal tracking, transportation, logistics, home and office, mood-based services, positioning, industrial and military applications. The technological improvements in wireless communiqué and micro-electronics have effected in a mounting attention in the area of wireless sensor area. A sensor network absorbs using a selection of sensors for dispersed monitoring of real time events. And the wireless networks have limited energy, as the sensor nodes are battery powered. The sensor nodes also have incomplete computational capability and memory that can be used in remote areas or in hospices. There is an increasing use of sensor networks for everyday life applications such as monitoring patients in hospitals and military applications. Such applications make it vital to have a good security infrastructure for sensor networks. And the deployment of these networks in applications like military applications, healthcare and the limited memory and power have made the plan of a security protocol very difficult. The safety measures of sensor networks can be given in numerous means. The end user accessing base station data may be averted from performing so in a number of means. Communiqué among the sensor motes and base station can be hunched. It will be achieved by analog or digital congestion of signals in the shape of (Denial of Service) attacks that has flooded the network. The targeted Denial of service attacks on strategic motes in the wireless sensor network also hunk communiqué of huge parts of the network with the base station. The communiqué between base stations and other sensor nodes are prohibited by taking up the wrong routing data so that the traffic goes to the erroneous loops or destination.

II. COMPARATIVE REVIEW

In recent years, the research of developing healthcare has attracted the people a lot. In this system we will develop the secure system for health data that has privacy of data by using the mechanism of secure key exchange mechanism.

In [4] WSNs appear to be a promising realization of the I o T. It is also believed that the synergy between WSN and Cloud Computing will over a potential solution to various social, environmental, public problems, e.g., the global energy crisis, population ageing, and security surveillance.In this author have identified the unique characteristics of WSN and Cloud Computing. This helps us to clear up some of the confusion over these buzz words, which in turn permits us to reveal the opportunities of applying one technology by leveraging another to tackle even more complex problems. We have also identified a number of challenges that we are facing, and we hope this can inspire researchers to investigate the potentially powerful combination of WSN and Cloud Computing.

In [2] the author explained that WBAN is the rising and hopeful knowledge which can alter individual's health-care

history revolutionarily. Information security and isolation in WBANs and in related e-healthcare area is a vital area, and in this still remain a variety of considerable confronts to overcome. The research in this area is still in its immaturity now, but we believe it will draw a large amount of interest in coming years.

In [8] the author has argued for the incorporation of sensor networks and Cloud Computing to carry the dynamic loads which are taken by surrounding applications. It has showed that how wireless networks can be merged with Cloud Computing to permit the offloading of resource-concentrated tasks to the Cloud. Experimentation was taken out to show the elastic nature of Amazon EC2 which can sustain the dynamic loads taken by these applications. In this situation, the Cloud will be employed to host image investigation structures that are able to identify suspect vehicles which police officers are searching for. As traffic raises, more models will be launched to provide a mechanism that can reliably recognize suppose vehicles even in high range of traffic.

In [11] authors proposed a technique to get secure access to outsourced information in owner-write-users interpret applications. It assumed that the data has a large scale and tried to decrease the transparency at the information owner and service giver. To encrypt each information wedge with a unique key so that cryptography based access control can be attained. By the acceptance of key derivation technique, the owner needs to uphold only a few secrets. Investigation shows that the key deri-vation process based on hash functions will give very less transparency. It examined the computational, storage, and communiqué transparency of the approach. We also investigate the scalability and safety of the approach. Extensions to our approach include the following aspects. First, we plan to design a new scheme for key management based on this approach so that it can be applied to many write-many-read applications. In this way, we can further reduce the number of keys that the owner sends to the end user. Finally, we plan to integrate existing approaches to access control, provable data possession, and key management for outsourced data to develop a new approach to secure Storage-as-a-Service.

TABLE 1: Comparative Review

Year of publication	Techniques	C Pros:	Cons:
2011	Unique C_H of Cc and WSN	H_D CP_{LX} P_{BLM}	I_{MM} R_{ST}
Feb 2010	E-H_C	$\mathbf{A}_{DC}$	C_{PLX}
Nov 2010	Computing method	A_{CC}	S_{CR}
2009	Encryption Based on hash functions	P_{ER}	S_{CR}

Where
Cc=Cloud computing; H_D=handle; C_{PLX}= complex; P_{BLM}=problem; P_{ER}=Performance; I_{MM}=immature; R_{ST}=result; H_C=healthcare; C_{PLX}=Complex; A_{DC}=Advance; S_{CR}=Security.

III. PROBLEM FORMULATION

In this part, we formulated architecture is described which enables a healthcare institution, like a hospital or a clinic, to direct data collected by WSN for patient supervision. The formulated architecture is scalable and is able to store the huge amount of data produced by sensors. As the data are highly susceptible, a new safety method to ensure data confidentiality, information integrity and the fine grained admittance control is formulated. Unlike active patient-centric systems, security configuration and key management in this are totally transparent to client and server (patients and doctors) and do not need their interventions. In order to get the objectives, a new architecture is proposed which takes two categories of users i.e. patients and doctors, and is made up of the given components:

(1) The WSN that takes health information from patients
(2) The examining uses that permits health takers to use the stored data
(3) The Health-care Authority (HA) which showed and enforced the safety terms of the healthcare organisation.
(4) The servers of cloud that have certain data storage.

Besides taking information on the cloud, this design proposes almost countless storage capability and high scalability. Certainly, this increases its storage capacity, by on-demand provisioning structure of the cloud, whenever it is essential. Additionally, it offers enormous convenience to the healthcare institution as it does not have to think about the complexity of servers' management.

To get fine grained admittance control, it makes use of attribute based encryption (ABE) to encrypt information before storing that on the cloud. Though, integrating ABE into medical systems is a big challenge. In ABE, data is encrypted with an access feature that is the logical expression of the access policy (eg: the information can be accessed by physician in cardiology division). The encrypted data can be decrypted by any client if his secret key has attributes that satisfy the access policy. The authority of ABE is that we do not need to rely on the storage server for evading unauthorized data access as the access policy is fixed in the cipher text itself. The next challenge in the integration of ABE was keys and access structures management. Certainly, the questions that who should generate the access structure that govern the security policy and who should generate and distribute keys necessary to access to the data is a big challenge in medical systems.

To answer these questions, existing ABE-based systems adopted a patient centric approach that we showed unsuitable for our application. To handle the first confront of ABE integration, we formulate to use both symmetric cryptography and ABE to encrypt data. More purposely, we used to encrypt every file with a randomly generated symmetric key (RSK) and encrypt the RSK with ABE. Finally, our solution has less encryption overhead compared to the naif utilization of ABE to encrypt the whole file. In fact, ABE consumes much more processing power than symmetric cryptography when we use complex access policy like ones used in medical systems.

To tackle the second challenge, which is mastering the complexity of security management, we introduce an entity that we call Healthcare Authority (HA). The HA ensures and implements the security policies of the medical organisation. It is used by the administrators of the healthcare institutions to define rules as"who can access to what". Based on these rules, the HA generates and sends to each user his ABE security parameters which are a pair of access structure and secret key. Introducing the HA releases users from creating and distributing access structures and secret keys. Consequently, it improves the system usability since a patient has no action to do to secure his data. Also, the healthcare professionals transparently access to data falling under their scope. In our process design, every patient has an own WSN possessed with a set of light weight/small sensor motes and a gateway.

A WSN enables inconspicuous and nonstop health check up of the patient at the hospice and at home settings. Sensor motes are taken by the patient to take different health data like heart beats, motion and physiological signals. Each mote sends the collected data via a wireless communiqué channel to the gateway. The gateway checks the different health data into a folder and encrypts it using the RSK. Thereafter, it sends the changed file along with the RSK encrypted using the access structure gained from the HA to the cloud. The monitoring application allows healthcare professionals to supervise their patients and enables them to access to a patient's data anytime and from everywhere using a computer or a Smartphone. The monitoring application downloads the required data from the cloud and decrypts it using its secret key.

IV. SUMMARY

In this proposed system, we addressed the challenge of data man-agement in wireless sensor networks for patient supervision. We proposed a secure and scalable architecture that leverages cloud computing technology to dynamically scale storage sources via on demand provisioning. Furthermore, we pro-posed an innovative security scheme that eliminates potential security threats of medical data outsourcing and guarantees confidentiality, integrity without involving patients or doctors interventions. To implement complex and dynamic security policies necessary to medical application, we developed a fine grained access control that combines attributes based encryption and symmetric cryptography. This combination reduced the management overhead and the encryption/decryption time as showed by our preliminary performance evaluation. In future works, we plan to use distributed attribute-based encryption to have multi healthcare authorities. Also, we plan to perform more thorough and complete performance evaluation during encryption, decryption and revocation.

V. REFERENCES

[1] H. Alemdar and C. Ersoy, "Wireless sensor networks for healthcare: A survey," Computer Networks, vol. 54, no. 15, pp. 2688–2710, Oct. 2010.

[2] M. Li, W. Lou, and K. Ren, "Data security and privacy in WBAN," IEEE Wireless Communications, vol. 17, no. 1,pp. 51–58, Feb. 2010.

[3] R. Buyya, S. Venugopal, C. S. Yeo, J. Broberg, and I. Brandic, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," Journal of Future Generation Computer Systems, vol. 25, no. 6, pp. 599–616, Jun. 2009.

[4] R. Liu and I. J. Wassell, "Opportunities and confronts of WSN using cloud services," in Proceedings of the workshop on Internet of Things and Service Platforms, IoTSP '11, New York, NY, USA, pp. 41–47 (2011).

[5] J. M. Gnanasekar, R. S. Ponmagal, V. Rajesh and P. Anbalagan, "Integration of WSN with cloud," in International Conference on Recent fashion in Information, Telecommunication and Computing, ITC'10, Kochi, India, pp. 321–323.(Mar. 2010)

[6] C. O. Rolim, F. L. Koch, C. B. Westphall, J. Werner, A. Fracalossi, and G. S. Salvador, "A cloud computing answer for patient's data col-lection in health care organisations," in Second International Conference on eHealth, Telemedicine, and Social Medicine,

ETELEMED '10, St.Maarten, Netherlands Antilles, pp. 95–99(Feb. 2010)

[7] W. Beer and W. Kurschl "Combining cloud computing and the WSN," in Proceedings of the 11th International Conference on Information Integration and Web-based Applications & Services, IIWAS '09, New York, NY, USA, 2009, pp. 512–518.(2009)

[8] D. Murray, K. Lee, D. Hughes, and W. Joosen, "Extending sensor networks into the cloud using amazon web services," in IEEE Inter-national Conference on Networked Embedded Systems for Enterprise Applications, NESEA'10, Suzhou, China, Nov. 2010, pp. 1–7.

[9] B. Song, M. M. Hassan and E. Huh, "The framework of sensor-cloud integration opportunities and challenges," registered in Proceedings of the 3rd ICUIMC '09, New York, NY, USA, 2009, pp. 618–626.(2009).

[10] L. T. Vinh, D. V. Hung, L. X. Hung,D. Guan, Z. Pervez, P. T. H. Truc, A. M. Khattak, M. Han, S. Lee, and Y. Lee, "Context-aware human activity recognition and decision making," in 12th IEEE International Conference on e-Health Networking, Health-com'10, Lyon, France, ,pp. 112–118.(Jul. 2010)

[11] Z. Li, R. Owens, W. Wang and B. Bhargava, " The Secure and efficient access to for data," registered in Proceedings of the ACM workshop on Cloud computing security, New York, NY, USA, 2009,pp. 55–66.(2009)