# Privacy and Security Mechanisms for eHealth Monitoring Systems

M. Ajmal Sawand
Sukkur Institute of Business Administration
Sukkur, Pakistan

Najeed Ahmed Khan
Computer Science and Software Engineering Department
NED University of Engineering and Technology
Karachi, Pakistan

***Abstract*—The rapid scientific and technological merging between Internet of Things (IoT), cloud computing and wireless body area networks (WBANs) have significantly contributed to the advent of e-healthcare. Due to this the quality of medicinal care has also been improved. Specifically, patient-centric health care monitoring plays important role in e-healthcare facilities by providing important assistance in different areas, including medical data collection and aggregation, data transmission, data processing, data query, and so on. This paper proposed an architectural framework to describe complete monitoring life cycle and indicates the important service modules. More meticulous discussions are then devoted to data gathering at patient side, which definitely serves as essential basis in achieving efficient, vigorous and protected patient health monitoring. Different design challenges are also analyzed to develop a high quality and protected patient-centric monitoring systems along with their possible potential solutions.**

***Keywords*—Wireless body area network; e-healthcare; mobile crowd sensing**

## I. Introduction

Cloud computing offers number of opportunities to the users and services providers includes providing facility for online computation and/or Google cloud storage outsourcing. Resulting of such technological merging, medical health care systems has benefited from these development. In particular the continuous miniaturization of devices has enabled the improvement of e-health monitoring systems. A number of cost effective sensors are now equipped in cellular phones, wearable devices around patient bodies. They work as important elements of WBAN [1]. Despite the recent technological advancements of WBANs, as well as their great potential to improve the quality of health monitoring, the performance with respect to energy efficiency, privacy and security is not sufficiently guaranteed.

Recent years comprehensive advancement in the smart phones sensors, wireless communications and body sensors have been observed. They are now commonly using with health monitoring systems and are provide efficient results. The health care monitoring tasks are now become persistent user friendly environment compared to the past traditional clinical environment. The variety of monitoring focuses significantly enlarged, varying from the patents at critical care, such as a patient in ambulance or the one with chronic diseases. In precise the body sensors installed around the patients body as well as the context-aware sensors those equipped in smart phones can also be used to measure the patients vital signs or vital health parameters such as temperature, heart rate, blood pressure etc.

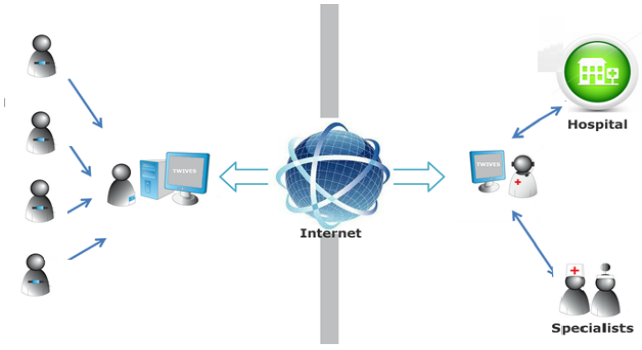


Figure 1: Health Monitoring System Architecture.

To describe explicitly an e-healthcare system, the proposed e-healthcare monitoring framework is shown in Figure 1. The figure 1, explains the following service components,

- *WBANs sensors*: ranging from IoT sensors to wearable sensors used to collect patients (required) data and transmit them to the computer, servers or gateways;
- *Relay communications networks*: ranging from short range wireless communications, cellular networks to wireline networks;
- *Data processing servers*: the data is processed and stored on cloud data centers, allowing clinic stuff or physicians to query in need.

It's clear that the quality of $e_health$ care services depend on on the seamlessly integration of the following three essential components includes;

- *Wireless communications technologies*
- *Energy efficiency*
- *Patient privacy*

Each of these is attract great efforts from both industry and academia and also considered the top concerns of e-health care services. For example, WBAN IEEE standard has become available in 2012 [25]. This paper focuses to investigate the key challenges for succeeding efficient, secure and reliable data collection of the patients that require more efforts. In the proposed framework, a variety of solutions tackling those recognized challenges and eventually proposes the potential

amalgamations of multidisciplinary approaches for developing a holistic e-health care oriented, cyber-physical system (CPS), patient-centric framework.

In particular, from the patient-centric perspective, the patients can be either individual or collective, depending on the scenarios. For example, WBANs could be more widely used for individual patient monitoring.

## II. Security Requirements in eHealth Monitoring Systems

This section describe the security requirements of the proposed ehealth monitoring system .

*1) Trusted Authority:* It is assume that this service component is associated with the cloud service provider. It generates public and secret key parameters for the proposed ehealth monitoring system. It is further assume that trusted authority is responsible for the issuing keys, updating them and revoking them. It also grants differential access rights to the individual users based on their attributes and roles.

*2) Cloud service provider:* Besides providing secure communication mechanism, cloud service provider felicitates with data storage, data processing and secure retrieval of the data based on the access privileges of the data access requesters..

*3) Registered User:* Patient who is registered to the trusted authority is considered as registered user. A registered user is responsible for defining attribute based access policy. Registered user defines who has to access his/her data.

This entity of the health monitoring system is registered with complete physical address (GPS location), telephone numbers and availability of the doctors and it will periodically update the information about doctors availability and their duty timings as well as number of stand by doctors.

*4) Data access requester:* Data access requester can be a doctor, a pharmacist, a researcher and hospital. Their access rights and mechanism is defined by the patient (generally) and whole mechanism is provided by the security provider, cloud service provider is that entity in our proposed scheme.

## III. Possible Security and Privacy Preservation Solutions

Our proposed multidisciplinary approach contains integration of WBANs, IoT and VSN (one sensor for multiple application and software sensor which is installed in smartphones) is designed to ensure efficient data delivery maintaining security and preserving privacy of all stakeholders. Since, this framework is designed to ensure pervasive, real time and secure data query in networks of medical sensors. Our extensive survey will felicitate to explore promising solutions related to the security, privacy preserving and energy efficient data transmission.

Emergence of the internet of the things have made systems more vulnerable. Privacy and the security of the systems have become pre-requisite for every service. There are a few already proposed solutions which ensure privacy and the security of the system. Secure authentication and access control surely improve the privacy and the security of the any system which has connection with internet. In this section, limited discussion of already suggested solutions for privacy preservation and access control is given i.e., hardware device authentication based physical unclonable functions and role based access control schemes respectively.

### A. Physical Unclonable Functions (PUFs)

Despite of the advancements in the technology, authenticity of the requester, sender or receiver of the data has consistently raised various issues. Most of the authentication mechanism is worked on the basis of the unique ID and various secret key protocols in the healthcare systems. Therefore, it is most important concern to store and preserve such secret keys and unique IDs of the all stakeholders and their devices. Moreover, their transportation among the all involved must also be efficient and more secure, so that malicious attackers could not any access to that data. Classical approaches of the storing secret keys and IDs include storing on the volatile storage of the chips or in the fusesor EEPROMS

The integrity of authentication schemes and encryption algorithms lies in a unique ID or a secret key. Hence it is imperative that these secret keys are generated and stored in a secure manner, protecting them from malicious attackers. Conventional approaches rely on storing the secret key in non volatile storage on chip, either in fuses or EEPROMs [10]. However, these approaches are vulnerable to the various types of the attacks because secret keys are permanently stored in the digital form which is definitely risky in the long term. Various methods like reverse engineering, optical and chemical methods can give access to the keys which are permanently stored in the forms of the already mentioned classical methods of the storage and preservation of the secret keys. Therefore, it is need of the time to prevent such attacks which can easily get access to the secret keys and IDs which are the basis of the whole security mechanism.

One of the potential authentication mechanism which can prove more secure in the ehealth monitoring systems is Physical Unclonable Functions (PUFs). It is assumed that all the devices used by medical staff and patients are working under mechanism of PUFs which is more secure alternative to digital keys. Each device used in our proposed system model is bound to a unique random unclonable function that serves as its identity. Physical Unclonable Functions can be enabled into smart cards of medical staff and patients personal servers (PDA/Smatphones) for secure and efficient authentication. A PUF is a physical pseudo-random function which is derived from the small variances in the wire and gate delays. These delays are unique for every hardware. Therefore, these are impossible to create duplication [11].

Mostly, information and the data of the patients is accessed either by the medical or clinical staff or researchers and sometimes government health ministry. Therefore, we assume that service cards of the all involved people who want to access the data are unclonable like VISA bank cards. Operational mechanism of PUF based authentication can be as follows: All smart cards have microchip with a PUF on it. Manufacturing of such cards creates a large set of challenges and their responses in the form of the challenge-response pairs for the future authentication. These pairs are stored in the very secure place. Each time, any one who is interested to access the sensitive

data of the patients must use that particular card, the card reader queries the card for the responses to a small set of challenges in the stored database. If that card gives proper response of the challenges means the authentication is granted and user is allowed to access the data. Hence, authentication of the requester or sender is verified.

### B. Proposed access control in health monitoring system

Medical data of the patients is more sensitive which needs strong security and tough authentication process in order to avoid any security breach in the data. Proposed design may include one of these two access control schemes, (1) Role Based Access Control and (2) Attribute Based Access control scheme. Here, a brief description of the both schemes is given and discuss which could be appropriate for our proposed health monitoring system.

*1) Role Based Access Control Scheme:* We assume that our security scheme is working on the mechanism of role based access control schemes. All stakeholders at clinical side are assigned roles to access patients data. For example, every patient has a particular doctor/specialist, he/she can access the sensitive data of the patient. Following is the brief description of the primary roles for the role based access control scheme (RBAC):

1) Role assignment: We assume that assignment of the role to the clinical staff is processed by the security providers (security system) which can be any server some where in the cloud
2) Role authorization: A clinical staff's active role (function) must be authorized for the clinical usage. With above role assignement, this rule ensures that individual who want to access data can take on only roles (functions) for which he/she is authorized.
3) Permission authorization: A clinical staff can exercise a permission only if the permission is authorized for the clinical staff's active role. With the previous two points (role assignment and role authorization), this role ensures that person who want to access the data can exercise only permissions for which he/she is authorized.

We further assume that one staff member can have various responsibilities (functions), similarly one function can be assigned to the multiple clinical staff members. In different situations, when a patient wants to encrypt his/her sensitive data, it is imperative that he/she must define and establish a specific access control policy which clearly and efficiently defines that who can decrypt his/her particular data. For example, patient is admitted in public hospital in Paris wants to send his/her confidential report to concerned doctor. The patient may want to encrypt a sensitive report so that only personnel that have certain roles or functions can access it. For instance, the patient may specify the following access structure for accessing this medical sensitive data: ((Public Hospital AND (Paris)) OR (Specialist Doctor) OR Name: Dr Johns). By this, the patient could mean that the report should only be seen by desired doctor named Dr Johns, who works at the public hospital Paris.

*2) Attribute Based Access Control Scheme:* The health related data is the most sensitive data of individuals which needs more secure and reliable access control mechanism to ensure maximum privacy. Usually, access to the data is patient centric means patients have the privileges to define access structure (who can access his/her data).

Sometimes, patients give access to their sensitive data to get assistance in the critical conditions. For example, they can disclose their location in order to get health care service at their desired location. Therefore, patients can define access tree depending on the different situations.

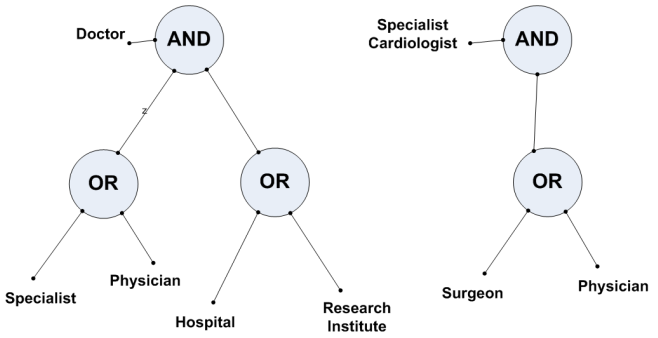


Figure 2: Example of data access control structure

We assume that there are three domains in this access control scheme: a central attribute authority, the patients and the doctors (physicians/specialists). Each doctor has particular privileges or rights to access patient data after proving their authenticity. Each doctor owns a set of privileges associated to his position such as position=specialist or physician, affiliation=Hospital or Research institute. Since, specialization can be of various types depends on the diseases of the patients. That can be cardiology, hypertension, diabetic etc. Specialist doctors and their attributes (functions) are assigned according to the diseases and condition of the patients. For example, personal and medical data of patients suffering from heart diseases is assigned to the specialists satisfying specialist=Cardiology and expertise=Surgeon or Physician can decipher the personal health information and verify his authentic identity. Figure illustrates the access structure in our proposed ehealth monitoring system. Since, The authority is responsible of issuing private keys corresponding to each attribute the doctors possess.

*Secure Communication Mechanism*:

WBAN sensors have low computational capability, storage and battery power. Traditional protocols like RSA are not suitable for such resource constraints networks. Moreover, various certificates like X.509 are also not suitable during TLS handshake due to their inappropriate size which proof expensive to transmit.

### C. Identity-Based Cryptography

For the security of the our proposed ehealth monitoring system, reliable security can be achieved through the formulation of the Identity Based Cryptography. Following is the brief definition of the IBC which can be taken into secure scenario of the ehealth monitoring systems. This scheme can be called

light weight it avoids using certificates which reduces the number of the messages to be exchanged during key exchange. Certificates are usually quite large which definitely put burden on the memory and the bandwidth. In IBC there is a Private Key Generator (PKG) which has replaced traditional Certification Authority (CA) used in Certificate-based cryptography [19]. It generates a secret key for each node based on its unique identity. All the nodes must contain these secret keys before their deployment in the netwok. It is generally assumed that PKG is a trusted party which is hard to be compromised. To ensure, proper security mechanism, IBC scheme is used for the proposed system architecture.

### D. Eliptic Curve Diffie-Helmann

The main security of the system relies on the secure and efficient transfer of the shared key before exchange of the messages between the sensor nodes and controller or between controller and server. This protocol is generally used between two stakeholders of the healtcare system (wireless body area network in our case). This key exchange protocol allows controller of the wireless body area network and server to agree on a shared key over an unsecure communication channel. More detailed description can be found in RFC 2631 [8]. This protocol is the alteration of eliptic curve public and private key pairs. Here, basic concept of exchange between the controller of the WBAN and the server is given, which goes as follows: Both stakeholders must have the same eliptic curve, eliptic curve is a generator, represented it by P which is a point on the curve. Moreover, each party should also have public and private key pairs denoted as dA and dB for the private part and QA and QB for the public part respectively. More concretly d is a randomly selected value and Q is calculated as $Q = d * P$. After the transmission of public keys between both parties (controller and the server) then they can calculate the shared key x as $xA = dA * QB$ and $xB = dB * QA$ respectively. It holds x=x=x because $dA * QB = dAdB * P = dB * dA * P = dB * QA$. After that some form of hash function is used on x to get the shared key [8]. This is mechanism which is followed for secure transmission of the shared key between two ends of the network.

### E. Eliptic Curves

Eliptic Curves are also used for the efficient and secure key exchange. Ecliptic curve can also ensure maximum secure of the key exchange in health monitoring systems. Eliptic Curves key exchange mechanism is considered as one of the small key exchange protocols. It is considered as efficient and light weight mechanism with respect to the RSA. It can provide same level of security with 128 bit, where as RSA achieve that level of security with 1024 bit. Eliptic Curves are the algebric concepts described by the equation: $y^2 = x^3 + ax + b$ and the points on the curves. It is generally believed that as long as discrete algorithm problem is still expensive and difficult to solve, eliptic curve cryptography can be considered as secure [16].

### F. Bilinear Pairing

Bilinear Pairing is also previously widely used mechanism for secure communication between two ends. This is also one the proposed security approach in our ehealth monitoring system. We give general and most classified definition of the Bilinear Pairing which is as follows: In simple words, Bilinear Pairing can be described as the agreement of two parties on a shared key without exchanging messages. Mathematically: Let G1 denoted a cyclic additive group of some large prime order q and G2 a cyclic multiplicative group of the same order. A pairing is a map $e : G1 \times G2 \rightarrow G2$ and has property of bilinearity, if *P,Q,R* $\in$ *G1* and a $\in$ $Z_d^*$ [...] $e(aP, Q) = e(P, aQ) = e(P, Q)^a$ [19].

## IV. Conclusion

In this paper, a comprehensive framework for advanced E-health system is presented by describing, in detail, the entire remote health monitoring life cycle. It is also highlighted the essential service components, with particular focus on data collection at patient side. The proposed multi-disciplinary approaches are expected to be more robust, efficient, and secure for health monitoring, compared to the existing health care systems. To ensure high efficiency of the proposed framework, the key challenges that need to be solved in order to develop efficient and secure patient-centric monitoring system are presented and analyzed. Moreover, some potential solutions to overcome the above challenges are discussed. Finally, this concise survey paper serves as the blueprint for the future work that aims to propose original and effective solutions in the E-health monitoring field.

## References

[1] K.A. Najeed, S. M Ajmal, H. Marium, K. Arwa, and T. Mehak, " Real Time Monitoring Of Human Body Vital Signs Using Bluetooth and WLAN," In *International Journal of Advanced Computer Science and Applications* , October. 2016

[2] A. Milenkovic *, C. Otto, E. Jovanov "Wireless sensor networks for personal health monitoring: Issues and an implementation " Journal of Computer Communication 2006, volume 29 pages 2521-2533.

[3] Alshamali et al.; ECG compression using wavelet transform and particle swarm optimization, Journal of Medical Engineering and Technology, Vol. 35, No. 34, 149153.

[4] D. Donoho. Compressed sensing, Information Theory, IEEE Transactions on, 52(4), 1289-1306, April 2006.

[5] E.Candes et al.; "An introduction to compressive sampling". Signal Processing Magazine, IEEE, 25(2):21-30, March 2008.

[6] E. Candes, The restricted isometry property and its implications for compressed sensing, Comptes Rendus Mathematique, vol. 346, no. 9-10, pp. 589592, 2008.

[7] E. Candes and T. Tao, Near-optimal signal recovery from random projections: Universal encoding strategies? IEEE Trans. Inf. Theory, vol. 52, no. 12, pp. 54065425, 2006.

[8] E. Rescorla "RFC 2631 - Diffie-Hellman Key Agreement Method", June 1999, http://tools.ietf.org/html/rfc2631

[9] Garth. Crosby, T. Ghosh, R. Murimi, C. Chin, "Wireless Body Area Networks for Healthcare: A Survey", International Journal of Ad hoc, Sensor and Ubiquitous Computing (IJASUC) Vol.3, No.3,Jun. 2012.

[10] G. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation", in ACM/IEEE Design Automation Conference, pages 9-14, 2007.

[11] G. Hammouri et al., "Novel PUF-Based Error Detection Methods in Finite State Machines" In *Proc. of ICISC '08*, Dec. 2008

[12] H. Rheingold, "Using Participatory Media and Public Voice to Encourage Civic Engagement, Civic Life Online: Learning How Digital Media Can Engage Youth", he MIT Press, 2008, pp. 97118.

[13] J. Burke, D. Estrin, M. Hansen, A. Parker, N. Ramanathan, S. Reddy, M. Srivastava "Participatory sensing, " In *Proc. of the 4th ACM Sensys Workshops*, 2006

[14] J. Liu; Z. Zhang; X. Chen, K. Kwak, "Certificateless Remote Anonymous Authentication Schemes for Wireless Body Area Networks, " Parallel and Distributed Systems, IEEE Transactions on , vol.25, no.2, pp.332,342, Feb. 2014

[15] J.A. Tropp et al.; "Signal recovery from random measurements via orthogonal matching pursuit". Information Theory, IEEE Transactions on, 53(12):4655-4666, Dec. 2007.

[16] Koblitz, "Elliptic curve cryptosystems". Mathematics of Computation 48 (177): 203209

[17] Nicholas D et al., "Piggyback CrowdSensing (PCS): energy efficient crowdsourcing of mobile sensor data by exploiting smartphone app opportunities". In *Proc. of In SenSys'13*, 2013

[18] R. Ganti, F. Ye, and H. Lei, "Mobile crowdsensing: current state and future challenges, " Communications Magazine, IEEE , vol.49, no.11, pp.32,39, Nov. 2011

[19] R. Mzid et al.; "Adapting TLS Handshake Protocol for Heterogenousv IP-Based WSN using Identity Based Cryptography", newblock In *Proc. the International Conference on Wireless and Ubiquitous Systems* , Dec. 2010 , 8-10 October 2010, Sousse, Tunis.

[20] S. Thomas "SSL and TLS Essentials - Securing the Web", Wiley Computer Publishing, USA 2000

[21] Waheed Bajwa et al.; "Compressive wireless sensing", in In *Proc. of IPSN'06*, 2008

[22] X. Li, R. Lu, X. Liang, and X. Shen, "Smart community: an internet of things application, " Communications Magazine, IEEE, vol.49, no.11, pp.68,75, 2011

[23] X. Liang et al. Enabling pervasive healthcare through continuous remote health monitoring, IEEE Wireless Communications, vol. 19, no. 6, 2012

[24] Z. Zhang, R. Ando, and Y. Kadobayashi, "Hardening botnet by a rational botmaster," In *Proc. of Inscrypt'08*, Dec. 2008

[25] 802.15.6-2012 - IEEE Standard for Local and metropolitan area networks - Part 15.6: Wireless Body Area Networks.