International Journal of Scientific Research & Engineering Trends
Volume 4, Issue 5, Sept-Oct-2018, ISSN (Online): 2395-566X

Security and Privacy Issues in EHR Systems Towards Trusted Services

M.E. G.Kavita
Department of CSE
Sri Muthukumaran Institute of Tech.
Chikkarayapuram, Chennai
Tamil Nadu,India

Asst.Prof. K.Bala
Department of CSE
Sri Muthukumaran Institute of Tech.
Chikkarayapuram, Chennai
Tamil Nadu,India

Abstract **-As of late saw an across the board accessibility of electronic medicinal services information record (EHR) frameworks. EHR were produced during the time spent treatment in therapeutic focuses, for example, healing facilities, centers, different establishments. With the end goal to enhance the nature of social insurance benefit, EHR could be shared by an assortment of clients, so noteworthy security ought to be delivering to make EHR commonsense. EHR framework not totally settled out the protection challenges. In this paper an orderly writing survey was led the protection issue in EHR and make sense of the utilized security models. Additionally a novel Context-mindful Access Control Security Model (CARE) is proposed to catch the situation of information interoperability and bolster the security basics of human services frameworks alongside the capacity of giving fine-grained get to control.**

Keywords- **Electronic health records, Systematic review, Privacy, Security regulations, Interoperability..**

I.INTRODUCTION

The across the board accessibility of pervasive medicinal wearable gadgets, for example, brilliant therapeutic sensors and the utilizing of restorative administration programming frameworks drove the upset of gathering social insurance information. In this specific circumstance, sensors and medicinal frameworks can be worked by exceptionally various associations to ceaselessly detecting patient information amid the restorative procedure. However, only authorized users such as medical stuff should have access to the collected health data as it almost always contains confidential and sensitive data.

In fact, several pieces of regulations and standards have been proposed to protect individual privacy. One can consider the HIPAA (Health Insurance Portability and Accountability Act of 1996) that provides data privacy for personal health care information, the European Information Protection Directive 95/46/EC, the GLBA (Gramm-LeachBliley Act, the Sarbanes-Oxley Act, and the EUs Safe Harbor Law [1].

These laws as a rule require strict safety efforts for sharing and trading wellbeing information, and inability to conform to them is emphatically endorsed, with serious punishments being forced. In this unique situation, electronic human services frameworks (EHRs) representative such standards and in this manner were ordered as security basic frameworks [2].

These frameworks are separated in one critical angle to different frameworks: The adjusting among classification and accessibility. The pressure between these objectives is clear: while all the patients information ought to be accessible to be shared and checked to convey proficient social insurance administrations for security reasons, part of the data may be considered confidential and must not be accessible. Clearly, reconciling between the pair goals should be achieved to provide the best possible care for patients.

Without a doubt, EHRs are continuous, tolerant focused frameworks that make information accessible and overseen by approved suppliers in an advanced configuration. Truth be told, EHR was based upon the norms of gathering information from patients and is made out of three principle parts: An arrangement of insightful physiological sensors with an individual server to assemble the indispensable signs, a heterogeneous system, and a remote social insurance server. In EHRs, clients might be a wellbeing information proprietor (i.e., patients) or a requester (i.e.).
Specialists or drug specialists), servers, thusly could be nearby or cloud servers that store, process and break down the accumulated wellbeing information [3,4]. Systems, then again, go about as the extension associating among patients and the restorative staff to

help the transmitting and sharing of information [4]. Fig.1 delineates the common engineering of EHR framework. In spite of the fact that of numerous advantages given by human services frameworks, by the by, there are powerless against an extensive variety of security dangers on account of their compactness and. In particular, dangers were risen at each level of the framework, for example: At information gathering level [5-10], At transmission level [11-14], and At capacity level [15-19]. These dangers were portrayed in Section III. Notwithstanding the previously mentioned dangers, a few patients stress while utilizing social insurance frameworks applications.

So, it is necessary to ensure patients feel fully confident to use the system and have their own privacy control over it [11]. To this end, in this paper, we conduct an in-depth survey study to analyze the healthcare system's security and privacy threats. Then, we propose a novel security model that captures the scenario of data interoperability and supports the security fundamental of EHR along with the capability of providing fine-grained access control [20].

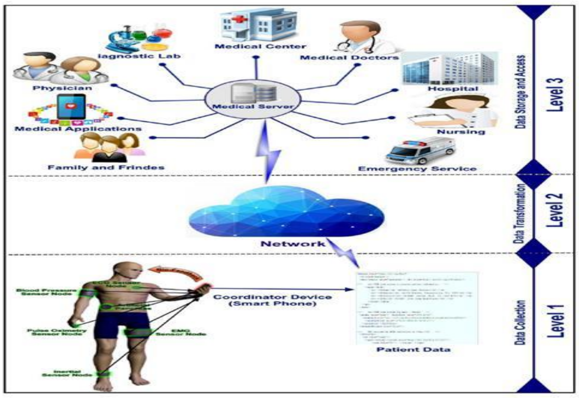

Fig.1 The architecture of Healthcare Monitoring System.

The remainder of the paper was organized as follows. In Section II, we discuss the privacy requirements of healthcare systems; its security attacks were then presented in detail in Section III. Section IV presents a set of exiting security models. The proposed model was discussed in Section V. Final conclusions, and the future work was offered in Section VI.

II.PRIVACY REQUIREMENTS IN HEALTH CARE SYSTEMS

Several general security and privacy requirements should be satisfied to provide the appropriate level of privacy in EHR system. Authors defined more than twenty security requirements that were found on surveys such as [3, 15-18]. Due to space limitations, we list the most important requirements:

- Access control is the ability to limit and control the access to resources by authorized users [3,21]. It makes use of three different security and privacy requirements: identification, authentication, and authorization. Identification is not an original security issue in itself, but its purpose is to identify users. Thus, it is used to affect the way a user can be authenticated [22,23,24]. Authentication, in turn, provides assurance that the requesting data access is authentic and valid and has the identity claims before accessing [21].
- It also ensures that the communication is with an authorized party on the other side [22]. Finally, the authorization process determines which part of data can be restricted to an external requester upon the security policy. It is important to mention that a proper access control mechanism should ensure patient privacy and also provide a good balance between availability and confidentiality [15, 23] security goals.
- Availability is the property of a system and resource being accessible, usable and available upon demand by authorized users [15,18,21] anytime anywhere in the healthcare system [25]. Ensuring availability also involves preventing service disruptions due to hardware failures, power outages, and system upgrade [16,22].
- Dependability guarantees easily retrievable of medical data at any time even if there are some threats caused by the network dynamic or failure node [18,16]. Usually in most medical cases, unable to retrieve accurate data is due to threats caused by the network dynamics, threaten the patient's life. Fault tolerance is a necessary requisite for dependability.
- Flexibility is to enable unauthorized participant who is not on the permissible list to access specific data in an emergency case to save the patient's life. Inability or prevention the access rules may threaten a patient's life [18].

III. SECURITY ATTACKS IN HEALTHCARE SYSTEM

Healthcare systems are vulnerable to penetration by malicious attacks or intentionally from users for profit. This damages the effectiveness or deterioration the performance of healthcare systems [4]. Specifically, insulin pump sensors, hospital networks, or the personal health data can be hacked or stolen by malicious users [19].

1.Assaults at information gathering level-These assaults may make a few dangers information accumulation level, for example, adjusting data, dropping some essential information, or resending information messages.

2.Jamming Attack-alludes to impedance assailant's radio flag with frequencies of the BAN (Body Area Networks). Bringing about confining and counteracting sensor hub inside the scope of the assailant signals for giving or accepting any message among the influenced hubs and other sender hubs as long as the sticking sign proceeds [5, 7].

3.Data Collision Attack-happens when at least two hubs endeavor to transmit all the while. Likewise, it alludes to sticking assaults when an enemy may deliberately create additional impacts by sending rehashed messages on the channel [6, 7]. At the point when the casing header is changed because of a crash, the mistake checking system at the less than desirable end recognizes that as a blunder and rejects got information. In this way, an adjustment in the information outline header is a risk to information accessibility in the BAN [5].

4. Information Flooding Attack-the assailant over and over communicate numerous solicitations to the injured individual hub for association until the point that utilizing all the intensity of its assets achieve a most extreme limit. causing a flooding attack [8].

5. Desynchronization Attack- in this type of attack, the attacker's tampers messages between sensor nodes by copy it many times using a fake sequence number to one or the two endpoints of a functioning association, which drives the WBAN to a limitless cycle, bringing about causing the sensor hubs transmits rubs again and squanders their vitality [6, 8]. Satirizing Attack where the assailant focuses on the steering data to play out a few disturbances, for example, ridiculing, adjusting, or replay the directing data, prompting confuse the system by making directing circles [9].

6.Specific Forwarding Attack- it happens when the aggressor pernicious hub in an information stream way advances chosen messages and drops the others. The harm ends up genuine when these vindictive hubs were found closeness to the base station [13]. Sybil Attacks: in Sybil, the assailant noxious hub speaks to in excess of one character in the system [6]. It has vital impact in geographic directing conventions.

Where the area data is required to be traded between the hubs and their neighbors to course the topographically tended to bundles proficiently [6, 13]. Tragically, identifying Sybil assailants are not effectively caught because of the capricious ways and high portability they utilize [4, 17]. **2. Attacks at transmission level-**These assaults may make a few dangers transmission level, for example, spying, adjusting data, interfering with correspondence, sending additional signs to obstruct the base station and systems administration activity.

2.1Eavesdropping of Patient's Medical Information: Monitoring system will record patient's health data from BANs to be transmitted to the healthcare providers. Unprincipled developers can easily build systems with the ability to spy on the patient's data through wireless technology. Thus the developer needs to apply controlling authority whenever they develop a system, which protects the patient's information against eavesdroppers and reduces the number of people who try to take and breach the patient's privacy [8, 11].

2.2 Man in the Middle Attacks-the attacker intercepts a communication between the end points and exchange messages between them. The communication is completely controlled by the attacker enable him being able to read, insert and modify the data in the intercepted communication [5, 12].

2.3 Data Tampering Attack-where a tampering attacker may damage and replace encrypted data by authorized network nodes [6, 13].

2.4 Scrambling Attacks- is a kind of jamming attack on radio frequency for short intervals of time during transmission of control or management information WiMAX frames to affect the normal operation of the network. It interrupts the communication that can prevent the patient's smart phone from sending data causing availability issue [5].

2.5 Signaling Attacks-Before patient's smart phone starts transmitting data, there is some preliminary signaling operation need to be performed with the serving base station. Signaling operations contain authentication, key management, registration, and IP-based connection establishment. The attacker can initiate a signaling attack on the serving base station by actuating extra state signals that block the base station. Thus, the excessive load on the base station results in DoS attacks, and the patient's smart phone cannot send data due to base station unavailability [5].

2.6 Unfairness in allocation-it lacks the network performance by interrupting the Medium Access Control (MAC) priority schemes [13, 14].

2.7 .Message Modification Attack- In this type of attack, the attacker can capture the patient wireless channels and extract the patient medical data to be tampered later, which can mislead the involved users (doctor, nurse, family) [8].

2.8 Hello Flood Attack-These types of attacks are used to fool the network. Where the attacker sends a hello message with a high powered radio transmission to the network to convince all nodes to choose the attacker for routing their messages [6, 13].

2.9 Data Interception Attack- this type of attack can take place via interception the patient's information by the attacker during exchanging them between computers of healthcare system through hospital LAN [5].

2.10 Wormhole Attack- this type of attack known as a silent and severe type of attack because it copies the packet at one location and replays them at another location or within the same network without any changes in the content. It aimed to damage the network topology and traffic flow through creating a tunnel between the two attackers to be used for transmitting between them [10,13].

3. Attacks at storage level-These attacks may cause several threats to storage level such as modifying patient medical information or changing the configuration of system monitoring servers.

3.1 Inference Patient's Information-Attackers try to combine authorized information and combine them with other available data, which leads them to identify sensitive patient data such as diseases [8, 11, 17]. Thus, patient's data should be anonymous to cover their identities or data before publishing/posting the data [3]. Unauthorized access of Patient Medical Information this type of attack can take place by unauthorized Individual without valid authentication, so patient's data will be accessed then it might cause problems such as damaging significant data [18]. Thus, it is necessary to protect patient privacy against breaching, capturing, and misusing by unauthorized users [11, 16].

3.2 Malware Attack- is a malicious software program designed to perform harmful actions [19]. This type of attacks has the ability to infect and propagate to the whole hospital server that can cause unavailability and disruption. Whereas, Changing and updating in software configuration of patient monitoring servers making system configuration unstable, resulting in system malfunctioning and communication interruption [5, 12].

3.3 Social Engineering Attacks- in this type of attack, a third party attacker can gain access to the system by fooling either the patient or authorized user to access the information. Here, authorized users can also disclose patient's data to concerned parties such as Health Insurance Company for unethical personal intends [5, 12].

3.4 Removable Distribution Media Attack-In this type of attacks it is possible to theft or loss computer or data storage medium, such as a USB flash drives, can be used to steal information and to propagate viruses in a healthcare monitoring system [5].

3.5 Others issues- several hardware and software issues can cause an interruption in the healthcare system. Hackers may develop new techniques or discover new software vulnerabilities. It is possible also that the system can be exposed to various types of software attacks such as viruses, worms, Trojans, and spyware attacks [19].

IV.E-HEALTHCARE SECURITY MODELS

To improve the quality of healthcare delivery, patient's data could be shared across a variety of users, which may lead to privacy disclosure. So, e-Health systems need to be protected through convenient security models to ensure proper access controls [19,9]. In fact, encryption is the traditional solution used. Although it provides a simple access control, it is not applicable for complex EHR systems that require various access requirements. That is, keeping the e-Health data secured is a big challenge due to two main reasons: the significant computational overhead when encryption techniques were used, and the sensitivity of personal medical information from changing when modification techniques are employed [30]. In this section, a detailed description of a set of security models, along with their corresponding levels, are presented.

1.Security Models for Data Collection Level-O. G. Morchon and K. Wehrle in [21] present a modular access control system for pervasive healthcare applications. The system extends the traditional RBAC model for two main issues: Firstly, to assign and distribute access control policies to sensor nodes. Secondly, to store the current medical context (location, time, health information) that influences access control decisions upon patient's medical situation (critical, emergency or normal situation). The modular design makes the system's configuration more effective and simplifies the composition of policies to deploy safer and more secure medical sensor networks. However, when a critical or emergency case raised, the medical stuff can override the restrictions to access sensitive data that was restricted in normal condition.

One of the limitations of this model is that there is no detection mechanism for unauthorized access when critical situations occur. A. Maw et al. [13] proposed an Adaptive Access Control model that provides fine-grained access control for medical data in BSNs and WSNs. The model considers privilege overriding and behavior, so users might be able to override a denial of access when unexpected events occur. Here, there is no need for a human effort to pay pass authorizations and policies since users initialize their sessions in behavior trust model based on users, location, time, and action. However, the main limitation of this model is that there is no prevention or detection mechanism to check user's data access when the critical situation occurs.

2. Security Models for Data Transmission Level Boonyarattaphan et al. [20] proposed a secure framework for authentication and data transmission using Encryption techniques for implementing two mechanisms: Data and Channel security. The channel security was provided by utilizing the SSL on the HTTP layer, while the data security is provided on the SOAP layer constructed above the HTTP.

They emphasized that RBAC should be used along with multi-factor authentication to guarantee proper authorization and authentication. Depend on the roles of stakeholders and data sensitivity; communication was divided into different layers where different authentication and encryption settings can be adapted.

The only limitation here is that it is dealt only with the web-based eHealth services.

N. Kahani et al. [18] proposed a new and secure scheme that supports both secure authentication and scalable fine-grained data access control. The scheme is based on a zero-knowledge protocol to verify and maintain the anonymity of the user's identity. This approach uses combination of a system public key and a secret session key generated by Derive Unique Key Per-Transaction (DUKPT) scheme to establish secure communication between different interacting entities. The access control mechanism was implemented in two phases: the first one utilizes a static authorization method to determine the highest access rights of users.

And, the second one grants the user the minimum access permissions on the required data according to the user's intention of access and the maximum rights determined by the first phase. To keep user's data confidential against malicious users and to decrease computational and communication overhead on data owners, data were stored in encrypted format in the cloud. However, by storing patient's health data in the cloud, patients loss the control over their data. Moreover, because of using encryption technique, it is difficult to achieve fine-grained access control to patient's data in a scalable and well-organized way.

Z. Guan et al. [19] considered the data security and privacy for cloud-integrated body sensor networks. They proposed a novel encryption outsourcing scheme named Mask-Certificate Attribute-Based Encryption (MC-ABE) by combining seven encryption algorithms. In this schema, data owner (patient) encrypts the outsourcing data to mask the row data before storing it securely in storage service provider (cloud servers). Furthermore, to achieve more effective access control, a unique authentication certificate is introduced for each user, which was verified before accessing data. Experimental results showed that the proposed scheme has less computation cost and storage cost compared with other common models. However, because of using encryption technique, it is difficult to achieve fine-grained access control, and still it requires some degree of computational overhead.

3. Security Models for Data Storage and Access Level- Lili Sun and Hua Wang [19] considered the notion of purpose to design a comprehensive usage access control model. Specifically, purpose notation was used for specifying privacy policies and giving the privilege to access private data. The proposed model consists of eight core components which are, subject attributes, objects, object attributes, rights, authorizations, obligations, and conditions. Whereas, authorizations, obligations, and conditions are components of usage control decisions used to determine whether a subject is allowed to access an object. The existence of obligations and conditions helped in solving certain shortcomings that have been common in access controls. That being said, the main limitation of this model is that it represents only a first step for authorization model in purpose data with usage control.

M. Barna et al. [1] proposed a security scheme based on different privacy levels. In short, the access control process was done in the centralized infrastructures. Here, the attribute-based encryption (ABE) was used rather standard way; privileges were mapped into roles and roles into ABE access structures. The data then is moved to the cloud-based storage, which enables the e-Health care service providers to decrease the overall maintaining cost of data and allows data to be online anytime and anywhere. However, because the data was stored in a centralized server, it becomes like a bottleneck when data requests were issued from different users.To solve the aforementioned problem,

L. Guo et al. [21] took into account the distributed nature of eHealth system when designing a privacy-preserving authentication system. In this system, instead of letting centralized infrastructures take care of authentication, the two end users (patients and physicians) do the authentication process. In particular, users are allowed to authenticate each other without disclosing their attributes and identities, which solves the problem of maintaining privacy and variability of each user's attributes.In the same vein,M. R. Kumar et al. [14] suggest a new patient-centric framework based on the same encryption technique (ABE).

Here, the users were categorized into two main domains namely: public and personal domains to face the key management complexity. In the public domain, users utilize multi-authority ABE (MA-ABE) to improve the fine-grained security countermeasures. While, in the personal domain, an owner is permitted to access/encrypt the data under his attributes. The limitations of this model is that integration ABE into large scale PHR system, required significant issues such as key management scalability, efficient on demand revocation, and lively policy updates which are nontrivial to resolve and remains up-to-date.

H. Zhu et al. [15] also proposed a secure and efficient personal scheme based on the attribute-based encryption (ABE) and re-encryption under the attribute group keys using RSA-Based proxy encryption. The proxy encryption technology is used to introduce an efficient privilege separation mechanism to ensure the validity of patients' data. Here, the write privilege keys were distributed to professional people and the read privilege

International Journal of Scientific Research & Engineering Trends
Volume 4, Issue 5, Sept-Oct-2018, ISSN (Online): 2395-566X

keys to patients, so that the data is not only fully controlled by the patient to authorize access, but also have the great validity. As a result, the computational overhead was reduced, and the key escrow problem was solved by employing re -encryption under the attribute group keys. Thus, the health provider could be prevented from obtaining the read keys without multiple-authority ABE.

V. Sunagar and C. Biradar [16] proposed a secured framework based on advanced encryption standard (AES) algorithm to encrypt every patient's data according to the security policy. AES enables the users to maintain data in a secured cloud environment. Ultimately, the framework consists of three modules: PHR Owner/patient module, Data confidentiality module, and Cloud Server module, which provides a high level of security.

Finally, W. Liu et al. [17] proposed a generic framework that depends on hierarchical identity-based encryption (HIBE) schema and the role-based access control (RBAC). While the HIBE is used to encrypt patients' data before outsourcing them to the storage server, the RBAC facilitates forwarding users' privileges. The experimental results of this model show that it is a practical solution to keeping data secure and confidential. However, the framework does not provide accurate access control requirements, as in some specific situations, patients might not have access to their own sensitive data (e.g., psychotherapy notes) without proper authorization according to HIPAA regulations. Such approaches suffer from the well-known encryption drawbacks [48].

V.CARE SECURITY MODEL

The Context-aware Access Control Security Model (CARE) architecture is based on the scenario of data interoperability and supports the security fundamentals of healthcare systems along with the capability of providing fine-grained access control. Specifically, the CARE model could be located on the healthcare server, which serves as an access point for users' requests. Fig.2 depicts the architecture of CARE.

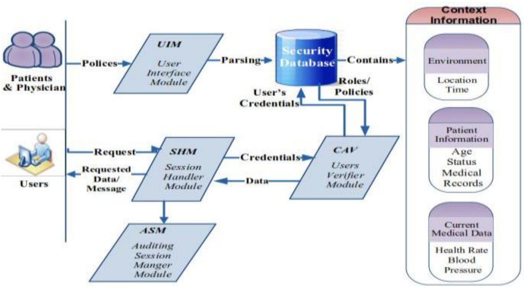

Fig.2 CARE Model Architecture.

1.In CARE, policies were defined by using the User Interface Module (UIM), which could be a website or a mobile application. Patients and physician define the policies together to save patients privacy. All the defined policies are then parsed into its components (e.g., constraints) and stored in a centralized security database, which is represented using an Extended-RBAC model. The ERBAC consists of roles, permissions, and users. Roles were created for various job functions, with permissions for specific operations.

Users are assigned particular roles, and through those role assignments acquire permissions to perform certain operations. The consolidation of access control for many users into a single role entry allows for much easier management of the overall system and much more effective verification of security policies. Three different types of context-data were considered in this model. The Environmental context refers to location or time, the Personal information context regarding age, status, or medical record and finally, the current medical data such as Heart rate or blood pressure [21].

2. Upon a user's request data, a session was established between the requester and the server side by the Session Handler Module (SHM). The requester's credentials (e.g., digital certificate, or user-name/password) were then extracted to be verified against a list of valid user accounts stored in the security database. The established session may involve more than one message, and are secured since secured transmission protocols were employed in all communications. It is important to mention here that session's information were saved to be able to communicate later. To this end, the Auditing Session Manger (ASM) takes this responsibility and states all the established sessions that could be used to retrieve multiple data for the subsequent access requests. This is opposed to stateless communication where it consists of independent requests (needs multiple authentications).

After establishing the session, the Users Verifier Module (CAV) verifies the requester credentials and then determines if the user is allowed to access the requested data or not. This is done by contacting the security database and retrieving the applicable policies and requester's assigned roles. CAV also classifies the request's cases as critical, emergency, or normal depending on the context -aware information and then adjusts the final access decision. In particular, when the patient's life is in danger the security settings are adapted by removing the need for user authentication to access the data.

VI.CONCLUSION AND FUTURE WORK

Patient's data should be kept securely in medical provider servers so that physicians can provide proper treatments. To ensure secure storage and access management, in this paper, we argue the security attacks in healthcare system along with the proposed security models that aim to prevent such attacks. Specifically, threats were categorized into three types depending on the its emerged level of the healthcare system, for instance: at data collection level; at transmission level; and at storage level. These attacks may cause several threats such as altering information, dropping some important data, interrupting communication, or sending extra signals to block the base station and increasing networking traffic.

After that, we briefly discussed a novel context-aware access control security model that supports the security fundamentals of healthcare systems and providing fine-grained access control. The model consists of multiple modules, each of which is in charge of taking a different type of task. This modular design aims at simple and efficient access control decision depending on the patient's situation and the requester's assigned roles.

ACKNOWLEDGMENT

The authors are grateful to the Applied Science Private University, Amman-Jordan, for the full financial support granted to cover the publication fee of this research article.

REFERENCES

[1]. Barua, M., et al. PEACE: An efficient and secure patient-centric access control scheme for eHealth care system. in Computer Communications Workshops (INFOCOM WKSHPS), 2011 IEEE Conference on. 2011. IEEE.

[2]. Fernández-Alemán, J.L., et al., Security and privacy in electronic health records: A systematic literature review. Journal of Biomedical Informatics, 2013. 46(3): p. 541-562.

[3]. Zhang, K. and X.S. Shen, Security and Privacy for Mobile Healthcare Networks. 2015.

[4]. Shinde, S.S. And D. Patil, Review On Security And Privacy For Mobile

[5]. Healthcare Networks: From A Quality Of Protection Perspective International Journal of Engineering Research-Online Peer Reviewed International Journal 2015. 3(6).

[6]. Habib, K., A. Torjusen, and W. Leister. Security analysis of a patient monitoring system for the Internet of Things in eHealth. in Proceedings of the International Conference on eHealth, Telemedicine, and Social Medicine (eTELEMED'15). 2015.

[7]. Saleem, S., S. Ullah, and K.S. Kwak, A study of IEEE 802.15. 4 security framework for wireless body area networks. Sensors, 2011. 11(2): p. 1383-1395.

[8]. CHELLI, K. Security Issues in Wireless Sensor Networks: Attacks and Countermeasures. in Proceedings of the World Congress on Engineering. 2015.

[9]. Kumar, P. and H.-J. Lee, Security issues in healthcare applications using wireless medical sensor networks: A survey. Sensors, 2011. 12(1): p. 55-91.

[10]. Saleem, S., S. Ullah, and H.S. Yoo, On the Security Issues in Wireless Body Area Networks. JDCTA, 2009. 3(3): p. 178-184.

[11]. Om, S. and M. Talib, Wireless Ad-hoc Network under Black-hole Attack. International Journal of Digital Information and Wireless Communications (IJDIWC), 2011. 1(3): p. 591-596.

[12]. Ramli, R., N. Zakaria, and P. Sumari, Privacy issues in pervasive healthcare monitoring system: A review. World Acad. Sci. Eng. Technol, 2010. 72: p. 741-747.

[13]. Partala, J., et al. Security threats against the transmission chain of a medical health monitoring system. in e-Health Networking, Applications & Services (Healthcom), 2013 IEEE 15th International Conference on. 2013. IEEE.

[14]. Niksaz, P. and M. Branch, Wireless Body Area Networks: Attacks and Countermeasures.

[15]. Bonab, T.H. and M. Masdari, Security attacks in Wireless Body Area Networks: Challenges And Issues. Academie Royale Des Sciences D Outre-Mer Bulletin Des Seances, 2015. 4(4): P. 100-107.

[16]. Santos-Pereira, C., et al. A secure RBAC mobile agent access control model for healthcare institutions. in Proceedings of the 26th IEEE International Symposium on Computer-Based Medical Systems. 2013. IEEE.

[17]. Zhang, R. and L. Liu. Security models and requirements for healthcare application clouds. in 2010 IEEE 3rd International Conference on Cloud Computing. 2010. IEEE.

[18]. Drosatos, G., et al., Towards Privacy by Design in Personal e-Health Systems. 2016.

[19]. Fatema, N. and R. Brad, Security Requirements, Counterattacks and Projects in Healthcare Applications Using WSNs-A Review. arXiv preprint arXiv:1406.1795, 2014.

[20]. Wellington, K., Cyberattacks on Medical Devices and Hospital Networks: Legal Gaps and Regulatory Solutions. Santa Clara High Tech. LJ, 2013. 30: p. 139.

[21]. Yu, S., et al. Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing. in INFOCOM, 2010 Proceedings IEEE. 2010.

[22]. Zubaydi, F., et al. Security of mobile health (mHealth) systems. in Bioinformatics and

Bioengineering (BIBE), 2015 IEEE 15th International Conference on. 2015. IEEE.
[23]. Nagaty, K.A., Mobile Health Care on a Secured Hybrid Cloud.
[24]. Kotz, D. A threat taxonomy for mHealth privacy. in COMSNETS. 2011.
[25]. Mare, S., et al. Adapt-lite: Privacy-aware, secure, and efficient mhealth sensing. in Proceedings of the 10th annual ACM workshop on Privacy in the electronic society. 2011. ACM.
[26]. Sun, L. and H. Wang. A purpose based usage access control model for e-healthcare services. in Data and Knowledge Engineering (ICDKE), 2011 International Conference on. 2011. IEEE.