ISSN 2348-1218 (print)
International Journal of Interdisciplinary Research and Innovations ISSN 2348-1226 (online)
Vol. 7, Issue 1, pp: (432-440), Month: January - March 2019, Available at: www.researchpublish.com

A Survey on Privacy issues in IoT based Healthcare Applications

Diana Moses

Professor, St. Peter's Engineering College, Hyderabad, India

Abstract: **Maturing of the populace brought about new difficulties for the general public and social insurance frameworks. Ambient Assisted Living (AAL) that relies upon Internet of Things (IoT) gives help to the debilitated individuals and backings their imperative day by day life exercises. Moderateness of and availability to AAL and the use of IoT begins changing human services administrations. This paper is an overview of the privacy and security issues in IoT human services applications for the crippled clients. Presentation incorporates meanings of privacy and security terms, and talks about their relationship. At that point, it displays an outline of the IoT, including its engineering and segments. Next, the paper indicates IoT-based answers for human services for the crippled, which is gone before by a exchange of the kinds of incapacities. A scope of IoT applications for the incapacitated clients is distinguished, and their characterization is proposed. At that point, privacy and security issues in these IoT applications are talked about, alongside IoT-based arrangements known in the writing. At long last, the Proposal distinguishes privacy and security prerequisites for IoT applications for the impaired clients.**

Keywords: **IoT, Healthcare, Disabled users, Privacy.**

I. INTRODUCTION

These days, Internet of Things (IoT) joins the Internet with sensors and a large number of gadgets, generally utilizing IP-based correspondences. In social insurance industry, IoT gives choices to remote observing, early counteractive action, and restorative treatment for systematized incapacitated. For IoT, individuals or articles can be outfitted with sensors, actuators, Radio-Frequency Identification (RFID) labels, and so forth. Such gadgets and labels encourage access by patients' guardians. For instance, RFIDs labels of patients or patients' close to home gadgets (counting medicinal gadgets) are meaningful, conspicuous, locatable, and controllable by means of IoT applications [2]. IoT empowers a wide scope of brilliant applications and administrations to adapt to difficulties that people or medicinal services area faces [3]. For instance, IoT has dynamic abilities to associate D2M (Device-to-Machine), O2O (Object-to-Object), P2D (Patient-to-Doctor), P2M (Patient-to-Machine), D2M (Doctor-to-Machine), S2M (Sensor-to-Mobile), M2H (Mobile-to-Human), T2R (Tag-to-Reader). This shrewdly associates people, machines, brilliant gadgets, and dynamic frameworks so as to guarantee a viable social insurance framework [1- 4].

Because of the expanding future, the gathering of individuals beyond 60 years old is expanding quicker than some other age aggregate [5]. This can be viewed as an accomplishment of general wellbeing approaches, wellbeing administrations and financial advancement. Be that as it may, it likewise shows a test to the society, which must adapt to a lot increasingly handicapped individuals. As indicated by the World Health Organization (WHO), the total populace of individuals beyond 65 2 billion 2050 years old billion by 2050 [6]. To abstain from overpowering wellbeing administrations, there is a genuine need to drag out free living of the crippled individuals (counting the debilitated older) at their very own homes. This enhances their personal satisfaction, yet in addition diminishes costs for their families and the general public on the loose.

Statistic changes require growing new functionalities and the coordinating new advancements into home conditions. Home computerization advances with the objective of enhancing personal satisfaction for the handicapped began to rise decades prior. They started with straightforward highlights identified with the robotization of fundamental errands, for example, lighting control utilizing movement indicators. In common method for mechanical advancement, more

intelligent and more astute frameworks of an ever more elevated multifaceted nature have and are being presented. The reconciliation of keen functionalities and Ambient Intelligence (AmI) at home outcomes in Ambient Assisted Living (AAL) situations that help care and give help to the impaired [7, 8]. Basically, similar frameworks with a few minor adjustment can also target a different population segment.

Ensuring privacy requires making sure that individuals maintain the right to control what information is collected about them, who maintains it, who uses it, how it is used, and what purpose it is used for.

1) Untraceability: Making it difficult for an adversary to identify that the same subject performed a given set of actions.

2) Unlinkability: Hiding information about the relationship between any items, such as subjects, messages, actions.

3) Unobservability: Hiding the fact that a message was sent (as opposed to hiding the identity of the sender of message).

4) Anonymity: Hiding information who performed a given action or who is described by a given dataset.

5) Pseudonymity: Using pseudonyms instead of using real identifiers.

II. LITERATURE SURVEY

A. IoT Architecture

The architecture of IoT consists of several layers, starting from the edge technology layer at the bottom to the application layer at the top, as shown in Figure 1 [9,10]. The two lower layers contribute to data capturing, while the two higher layers are responsible for data utilization in applications. The functions of the layers (from the bottom up) are as follows:

Edge technology layer (a.k.a. perception layer): This is a hardware layer which includes data collection components—such as wireless sensors networks (WSNs), RFID systems, cameras, intelligent terminals, electronic data interfaces (EDIs), global positioning systems (GPS). These hardware components provide identification and information storage (e.g., via RFID tags), information collection (e.g., via sensor networks), information processing (e.g., via embedded edge processors), communications, control and actuation (e.g., via robots). RFID systems are the most important components of IoT. They enable data transmission by a highly portable device called an RFID tag. An RFID reader reads the tag and processes the obtained data according to the needs of a specific application. RFID systems can be used to monitor healthcare objects in real-time, without the need of being in the line of sight. Data transmitted by the tag may provide disabled or device identification, disabled information (age, sex, blood pressure, glucose level, etc.), or location information [11]. Wireless sensor networks (WSNs) may consist of a large numbers of sensing nodes, which report the sensing results to special nodes called sinks [10].

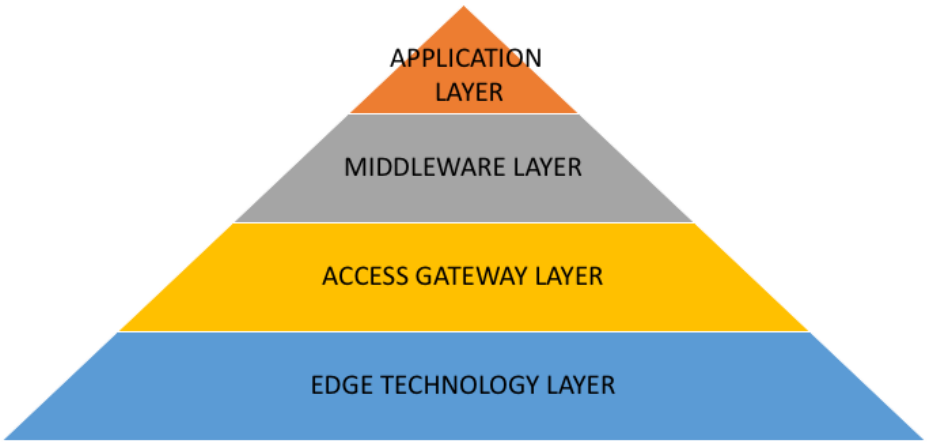

FIGURE 1: ARCHITECTURE OF IOT SYSTEMS

Access gateway layer (a.k.a. network layer or transport layer): This layer is responsible for data handling, including data transmission, message routing, and publishing and subscribing messages. It sends to the middleware layer information received from the edge layer, using communications technologies such as Wi-Fi, Li-Fi, Ethernet, GSM, WSN, and WiMax [9].

Middleware layer: It is a software platform that provides abstraction to applications from things. Also, it offers many services such as device discovery and management, data filtering, data aggregation, semantic data analysis, access control, and information discovery (using Electronic Product Code (EPC), or Object Naming Service (ONS)).

Applications layer: This top layer. It is responsible for delivery of various applications to different IoT users. It consists of two sub-layers [7]: a) Data management sub-layer: It provides directory service, Quality of Service (QoS), cloud-computing technologies, data processing, machine-to-machine (M2M) services, etc. b) Application service sub-layer: It is responsible for interfacing to end users and enterprise applications running on top of the IoT applications layer.

B. IoT in Healthcare

The healthcare business is in a condition of extraordinary misery. Healthcare administrations are costlier than at any other time, worldwide populace is maturing and the quantity of perpetual maladies are on an ascent. What we are drawing closer is where essential healthcare would end up distant to the vast majority, an expansive segment of society would go useless attributable to seniority and individuals would be progressively inclined to unending malady. Is it true that it isn't the apocalypse we suspected? Whatever, IoT application improvement is at your salvage. While innovation can't prevent the populace from maturing or destroy constant infections on the double, it can at any rate make healthcare simpler on a pocket and in term of openness.

Restorative symptomatic devours a huge piece of medical clinic bills. Innovation can move the schedules of restorative checks from a medical clinic (emergency clinic driven) to the patient's (home-driven). The correct conclusion will likewise reduce the need of hospitalization. Another worldview, known as the Internet of Things (IoT), has a broad material in various zones, including healthcare. The full use of this worldview in healthcare zone is a shared expectation since it enables restorative focuses to work all the more capability and patients to get better treatment. With the utilization of this innovation based healthcare strategy, there are unparalleled advantages which could enhance the quality and productivity of medications and in like manner enhance the wellbeing of the patients.

Concurrent alerts and observation

Continuous observing by means of associated gadgets can spare lives in occasion of a medicinal crisis like heart disappointment, diabetes, asthma assaults, and so forth. With continuous checking of the condition set up by methods for a brilliant restorative gadget associated with a cell phone application, associated gadgets can gather therapeutic and other required wellbeing information and utilize the information association of the cell phone to exchange gathered data to a doctor. Focus of Connected Health Policy directed an examination that demonstrates that there was a half decrease in 30-day readmission rate as a result of remote patient observing on heart disappointment patients. The IoT gadget gathers and exchanges wellbeing information: circulatory strain, oxygen and glucose levels, weight, and ECGs.

End-to-End availability and moderateness

IoT can robotize tolerant consideration work process with the assistance healthcare portability arrangement and other new advances, and cutting edge healthcare offices. IoT empowers interoperability, machine-to-machine correspondence, data trade, and information development that makes healthcare administration conveyance successful. Availability conventions: Bluetooth LE, Wi-Fi, Z-wave, ZigBee, and other current conventions, healthcare work force can change the manner in which they spot sickness and illnesses in patients and can likewise improve progressive methods for treatment. Thusly, innovation driven setup cuts down the expense, by chopping down superfluous visits, using better quality assets, and enhancing the assignment and arranging.

Information combination and analysis

Tremendous measure of information that a healthcare gadget sends in a brief timeframe attributable to their ongoing application is difficult to store and oversee if the entrance to cloud is inaccessible. Notwithstanding for healthcare suppliers to get information starting from numerous gadgets and sources and investigate it physically is an extreme wagered. IoT gadgets can gather, report and examinations the information progressively and slice the need to store the crude information. This all can happen overcloud with the suppliers just gaining admittance to conclusive reports with charts. In addition, healthcare activities enable associations to get crucial healthcare examination and information driven bits of knowledge which accelerate basic leadership and is less inclined to blunders. On-time alert is basic in occasion of perilous conditions. IoT enables gadgets to accumulate crucial information and exchange that information to specialists

for constant following, while at the same time dropping notices to individuals about basic parts by means of versatile applications and other connected gadgets.

Remote medicinal help

In occasion of a crisis, patients can contact a specialist who is numerous kilometers away with a keen versatile applications. With versatility arrangements in healthcare, the surgeons can quickly check the patients and distinguish the infirmities in a hurry. Likewise, various healthcare conveyance ties that are anticipating to manufacture machines that can circulate tranquilizes based on patient's remedy and sickness related information accessible by means of connected gadgets. IoT will Improve the patient's consideration In medical clinic. This thusly, will cut on individuals' scope on healthcare.

C. Challenges of IoT in Healthcare

Information security and privacy

A standout amongst the most critical dangers that IoT presents is of information security and privacy. IoT gadgets catch and transmit information in real-time. Be that as it may, the greater part of the IoT gadgets need information conventions and models. Notwithstanding that, there is critical equivocalness with respect to information possession control. Every one of these elements make the information very defenseless to cybercriminals who can hack into the framework and bargain Personal Health Information (PHI) of the two patients just as specialists. Cybercriminals can abuse patient's information to make counterfeit IDs to purchase medications and restorative gear which they can move later. Programmers can likewise document a false Insurance guarantee in patient's name.

Integration: various gadgets and conventions

Integration of various gadgets additionally causes prevention in the usage of IoT in the healthcare segment. The explanation behind this impediment is that gadget producers haven't achieved an accord with respect to correspondence conventions and standard. In this way, regardless of whether the assortment of gadgets are associated; the distinction in their correspondence convention confuses and obstructs the procedure of information conglomeration. This non-consistency of the associated gadget's conventions backs off the entire procedure and decreases the extent of versatility of IoT in healthcare.

Information over-burden and exactness

As examined before, information total is troublesome because of the utilization of various correspondence conventions and guidelines. Be that as it may, IoT gadgets still record a huge amount of information. The information gathered by IoT gadgets are used to increase essential bits of knowledge. Be that as it may, the measure of information is tremendous to the point that getting bits of knowledge from it are ending up amazingly troublesome for specialists which, at last influences the nature of basic leadership. Additionally, this worry is ascending as more gadgets are associated which record an ever increasing number of information.

III. EHEALTH REALITY

Inside the by and large associated healthcare and eHealth picture, increasingly incorporated methodologies and advantages are looked for with a job for the supposed Internet of Healthcare Things (IoHT) or Internet of Medical Things (IoMT). The period from 2017 until 2022 will be imperative in this progress, with a few changes previously 2020. From 2017 until 2022, development in IoT healthcare applications is undoubtedly ready to quicken as the Internet of Things is a key segment in the computerized change of the healthcare business and different partners are venturing up their endeavors. Besides, there is an expanding cognizance and commitment of shoppers concerning their health, interest for remote and home conceivable outcomes continues developing, different healthcare biological system players think of novel methodologies and organizations; and healthcare use decrease remains a principle objective, alongside better quality consideration. An increasingly incorporated and IoT-empowered eHealth approach demonstrates fundamental in every one of these territories.

Outside of this extension there is significant development ahead in an increasingly Industrial Internet of Things setting, whereby healthcare suppliers, for example, emergency clinics, influence IoT, in mix with applications and advancements in the field of robotics, man-made consciousness and Big Data. The second center zone of IoT applications we referenced

in the presentation (monitoring, following, upkeep, etc) is surely likewise going to continue developing; yet at contrast paces, contingent upon the medical clinic, nation, etc. Some will begin with following anything from medical hardware and patients to clinic building resources and beds, others will move to the following stages. In a health information setting accepted very a few information from medical gadgets and monitoring systems at last end up in Electronic Healthcare Records (EHR) Systems or in explicit applications which are associated with them and send the information to labs, specialists, attendants and different gatherings included.

As health-related information is gathered and progressively is accessible in real-time, it gets incorporated with electronic healthcare records (EHR). Real-time Health Systems (RTHS) will be a key zone for IoT in healthcare as Big Data Analytics instruments and procedures are used to assess both dynamic and static information for prescient examination as a component of far reaching healthcare systems enhancement programs. (Mind Commerce, end 2016. EHR systems are a long way from ubiquitous and most have not been planned with the Internet of Things, RFID and real-time information at the top of the priority list; they have been structured, if everything is great, to make healthcare quicker, increasingly quiet driven, progressively reasonable and better from the point of view of the patient's health and crafted by healthcare professionals, in light of rather static information.

These results are additionally basic in numerous IoT use cases in healthcare, yet they are not generally accomplished. Also, there are such huge numbers of ways to deal with the digitization of healthcare records that by and by an Internet of Things organization needs to consider these distinctions in the event that it is connected with an individual patient. Not all health information from associated gadgets at last grounds in the EHR/EMR condition. There are a lot of other data systems and systems of knowledge, contingent upon sort of information, gadget, extension and reason. In addition, there is a move towards Real-Time Health Systems (RTHS), which go past EHR and incorporate mindfulness and real-time information abilities in an IoT and associated/wearable gadget point of view. EHR systems are a piece of the more extensive setting and procedures inside this RTHS systems approach.

In addition, security and privacy by configuration should be a piece of any IoT use case, undertaking or arrangement. Utilizing the IoT and information means to enhance and decrease mistakes and expenses. Ensuring it doesn't get uncovered or utilized for the wrong reasons is critical. As referenced in different articles, individual healthcare information should be dealt with uniquely in contrast to a security and consistence point of view. Exceptional consideration for individual information in healthcare IoT ventures required. Different directions over the globe drive the consistence plan, yet healthcare information security needs to go past consistence. In the meantime, healthcare associations need to give careful consideration to consistence too, surely in districts where stricter controls are being established, for example, the EU GDPR where individual health information, just as hereditary and other medical and organic information, get uncommon consideration and are viewed as delicate. Plainly any IoT venture which includes individual health information, needs to take these guidelines and the legitimateness, plan, and dispersion stipulations, to give some examples, into record. Truly, any IoT task ought to have security and privacy by configuration at the top of the priority list where it concerns individual information. Nonetheless, the situations with respect to the assurance and influence of health information is, to say it somewhat, altogether different in the event that you begin looking at activities and controls over the globe.

IV. PRIVACY ISSUES IN IOT HEALTHCARE

These results are additionally basic in numerous IoT use cases in healthcare, yet they are not generally accomplished. Also, there are such huge numbers of ways to deal with the digitization of healthcare records that by and by an Internet of Things organization needs to consider these distinctions in the event that it is connected with an individual patient. Not all health information from associated gadgets at last grounds in the EHR/EMR condition. There are a lot of other data systems and systems of knowledge, contingent upon sort of information, gadget, extension and reason. In addition, there is a move towards Real-Time Health Systems (RTHS), which go past EHR and incorporate mindfulness and real-time information abilities in an IoT and associated/wearable gadget point of view. EHR systems are a piece of the more extensive setting and procedures inside this RTHS systems approach. In IoT applications for the impaired clients, gigantic measures of health information should be accumulated and investigated. Questions emerge who possesses the medical information for a debilitated, who has the directly to get to it, and where the crippled's information are put away? [11-13]. In this segment we tends to the most widely recognized privacy issues in IoT applications for the impaired clients alongside IoT-based arrangements that are known.

ISSN 2348-1218 (print)
International Journal of Interdisciplinary Research and Innovations ISSN 2348-1226 (online)
Vol. 7, Issue 1, pp: (432-440), Month: January - March 2019, Available at: www.researchpublish.com

Challenges in Patients' Privacy Exposure

A Personal Health Record (PHR) is "an individual electronic record of health-related data that adjusts to the broadly perceived interoperability benchmarks. PHR can be drawn from different sources while being overseen, shared and constrained by the individual" [14]. PHRs are accounted for to the e-health focus straightforwardly, and the essential privacy and security issue is to keep the patients' PHRs secret. Li et al. [15] proposed a strategy to scramble each PHR with one-to-numerous encryption strategies, for example, the ABE system, before re-appropriating it. Encryption calculations, for example, AES and MD5, together with proficient key administration, have been utilized to encode each PHR document [16,17]. A health framework can be isolated into two security areas, to be specific open spaces (PUDs) and individual spaces (PSDs), as indicated by the diverse clients' information get to necessities. PUDs comprise of clients who need get to dependent on their professional jobs, for example, specialists, attendants and medical analysts. Practically speaking, a PUD can be mapped to an autonomous financial area, for example, healthcare, government or protection divisions. For each PSD, its clients are by and by related with an information proprietor, (for example, relatives or dear companions), and they make gets to PHRs dependent on access rights allocated by the proprietor. Ukil et al. [18] presents a privacy estimation plot that identifies and investigates delicate substance of time-arrangement sensor information. It gauges the measure of privacy, to settle on a choice whether to discharge private information or not. The measure of the privacy can be characterized as follows:

$$\gamma_{s,v} = \rho_{\mathrm{M}} = \frac{\sum_{i=1}^{|v|} pr(v_i)\log_2 \frac{1}{pr(v_i)}}{\sum_{i=1}^{|s|} pr(S_i)\log_2 \frac{1}{pr(S_i)}}$$

where v is the sensitive part of S (sensor data set) and γ is the non-sensitive – part $S = v \cup \gamma$

Cyber-Attacks on Privacy

Digital assaults can infuse false information into a framework, causing basic harm in IoT applications. It is principal to give the sufficient dimension of assurance against digital assaults in brilliant home applications for the debilitated. In any case, the asset compelled nature of a considerable lot of IoT gadgets present in a shrewd home condition don't permit to execute the standard security arrangements. Tajer et al. [19], proposed a structure that ensures recognition of the digital assaults and recouping from them. Distinctive controlling operators, disseminated over the system, establish the assault identification subsystem. Framework recuperation includes iterative neighborhood preparing and message passing. Nguyen et al. [20], proposed another circulated digital assault recognition calculation, in light of the choice cost minimization procedure. It is demonstrated that is an appropriate answer for recognition of both known and obscure digital assaults.

Information Eavesdropping and Data Confidentiality

For the most part, the health information of patients, including the incapacitated, are held under the legitimate commitments of privacy, and made accessible just to the approved parental figures. It is essential to keep taking information from capacity or listening stealthily on them while they stream over the remote connections. For instance, a prominent IoT-based debilitated glucose monitoring and insulin conveyance framework uses remote correspondence joins, which are as often as possible used to dispatch privacy assaults. Information listening in may make harm the incapacitated by rupturing the crippled's privacy. Li et al. [21] propose moving code cryptographic conventions and body-coupled correspondence to moderate the listening stealthily on incapacitated's health information. Miaou et al. [22], propose a bi-polar different base information concealing strategy for pictures, where a pixel esteem distinction between a unique picture and its default JPEG lossy decompressed picture is taken as the number transformation base. The calculation permits to stow away, e.g., specialists' advanced seals and PHR inside a still picture. (The specialists' advanced seals are fundamental to the confirmation of PHR.) The still picture could be a logo of a medical clinic recognizing where the PHR originates from. A demonstrative report and a biomedical flag, for example, an electrocardiogram (ECG), can likewise be covered up in a picture. The proposed methodology permits concealing different information types in a similar picture. Every one of these information can be isolated and reestablished impeccably by the expected clients [22].

Information privacy can be enhanced by utilizing Public Key Encryption (PKI). PKI makes a powerful way to deal with information encryption as it can give abnormal state of certainty to trading data in an uncertain domain. Atzori et al. [10] presents an applied plan and a model execution of a framework dependent on IoT portals that total health sensor information and resolve privacy issues through computerized testaments and PKI information encryption.

Character Threats and Privacy of Stored Data

Loss of a patient's privacy, particularly her character information may result in critical physical, money related, and enthusiastic mischief to the patient. Slamanig and Stingle [23] present components for anticipating divulgence assaults:

1) Unlinkability: A framework containing n clients gives unlinkability if the connection of a report Di and a client Uj exists with likelihood p = 1/n. Subsequently, an insider or assailant can not increase any data on connections among clients and records by methods for exclusively watching the framework.

2) Anonymity: It is the condition of being not recognizable inside a lot of subjects X. The level of obscurity can be estimated by the measure of the namelessness set |X|. For instance, secrecy is given when mysterious client in a set U′ ⊆ U can get to report Dj.

3) Identity the board: A client's personality can be overseen by partitioning the character of an individual into sub-characters I = {Ipub , I1 , . . . , Ik }, where each the sub-personality is a client picked nom de plume. A client can allot any sub-personality for any subset of his PHR/EHR records. This permits her for concealing delicate information by means of a sub-character, along these lines shielding them from revelation assaults.

Uncovering put away PHRs can cause misfortunes of patients' privacy, particularly her character information. Namelessness and pseudonymity administrations can be utilized to shroud the real personality that is fixing to the put away information. Privacy administrations can ensure securing records by utilizing differential privacy strategies that depend on adding clamor to patients' records [24]. This might be utilized to guarantee that a database permits recovering just factual information, for example, total, normal, check, and so forth.

Location privacy

Area privacy is worried about area privacy dangers and listening stealthily on a client's area. Area privacy in WSNs, explicitly concealing the message sender's area, can be accomplished through steering to an arbitrarily chosen halfway hub (RRIN) [25]. Evesdropping and following of parcels can be avoided by the Location Privacy Routing (LPR) convention, which consistently appropriates the bearings of approaching and active traffic at sensor hubs [26].

Apparition single-way directing makes guarantees that bundles achieve the Base Station (BS) following distinctive ways so that each parcel made by a source pursues an alternate arbitrary way toward the BS [27]. The privacy issues in IoT healthcare applications alongside their IoT-based arrangements are condensed in Table 1.

TABLE I: PRIVACY ISSUES IN IOT-BASED HEALTHCARE SYSTEMS

Privacy Issues	IoT-based Solutions
PHRs exposure	Encryption before outsourcing, dividing health system into domains, analyzing sensitive data to be private or not
Cyber attacks	Detection methods and system recovery
Data eavesdropping and data confidentiality	Data hiding and cryptographic techniques
Identity threats and privacy of stored data	Pseudonymization of medical data, identity management, anonymity
Location privacy	Security protocols

V. CONCLUSION

The ongoing improvements in the zone of Internet of Things (IoT) demonstrate an extraordinary guarantee for giving answers for healthcare, including healthcare for the handicapped individuals. Be that as it may, there are numerous privacy and security challenges in IoT healthcare applications for the debilitated clients. This Thesis talks about IoT, its layered design, and its job in the healthcare business. It depicts privacy and security benefits, and proposes seeing secrecy as the crossing point of privacy and security. The Thesis presents IoT parts with regards to the IoT engineering, and for the most part from the security and privacy point of view. The paper recognizes the kinds of incapacities and arranges the regarding their versatility. It depicts the scope of IoT healthcare applications for the impaired alongside their order. It researches privacy and security issues in IoT healthcare applications for the impaired, and surveys IoT-based arrangements known.

REFERENCES

[1] A.J. Jara, M.A. Zamora, and A.F.G. Skarmeta, "(HWSN6) Hospital Wireless Sensor Networks based on 6LoWPAN technology: mobility and fault tolerance management, " 7th IEEE/IFIP Int. Conf. on Embedded and Ubiquitous Computing, vol. 2, Vancouver, Canada, Aug. 2009, pp.879-848.

[2] R. Tesoriero, J.A. Guled, M.D. Lozano, and V.M.R., Penichet, "Tracking Autonomous Entities using RFID Technology ," IEEE Trans. on Consumer Electronics, vol. 55 (2), May 2009, pp. 650-655.

[3] Giusto, A. Iera, G. Morabito, and L. Atzori, "An Overview of Privacy and Security Issues in the Internet of Things, "The Internet of Things, 1st Ed., Springer, New York, 2010, pp. 389-395.

[4] P. Yang, W. Wu, M. Moniri, and C.C. Chibelushi, "Efficient Objects Localization Using Sparsely Distributed Passive RFID Tags," IEEE Trans. on Industrial, vol. 60(12), Dec.2013, pp.1-11.

[5] U.S Department of Health and Human Services. Last access Oct. 12, 2014. Available on: http://www.hhs.gov/

[6] World Health Organization. Last access Oct. 12, 2014. Available on: http://www.who.int/topics/aging/en/index.html,

[7] H. Steg, H. Strese, C. Loroff, J. Hull, and S. Schmidt, "Europe Is Facing a Demographic Challenge - Ambient Assisted Living Offers Solutions," VDI/VDE/IT, Berlin, Germany, 2006, pp. 26-33.

[8] A.J. Jara, M.A. Zamora, and A.F.G. Skarmeta,"An ambient assisted living system for telemedicine with detection of symptoms," Bioinspired Applications in Artificial and Natural Computation 3rd Int. Work-Conf. on the Interplay Between Natural and Artificial Computation, 2009, pp.75-84.

[9] G. Santucci, "From Internet to Data to Internet of Things," Proceedings of the Int. Conf. of Future Trends of the Internet, J. Wireless Personal Communications, vol. 58(1), May 2011, pp. 49-69.

[10] L. Atzori, A. Lera, and G. Morabito,"The Internet of Things: A Survey," Computer Networks, vol. 54(15), Catania, Italy, 2010, pp.1-17

[11] C. M. Medaglia and A. Serbanati,"An overview of privacy and security issues in the internet of things", In Proc. of 20th Tyrrhenian Workshop on Digital Communications, Italy, 2010, pp. 389-395.

[12] L Brown and A.A. Adams," The Ethical Challenges of Ubiquitous Healthcare," Int. Rev. of Information Ethics, vol. 8, Dec. 2007, pp.53–60.

[13] K.D. Mandl, P. Szolovits and I.S. Kohane, "Public Standards and Patients', Control: How to Keep Electronic Medical Records Accessible but Private, BMJ, vol. 322, Feb. 2001. pp. 283-287.

[14] J.S. Khan, V. Aulakh, and A. Bosworth," What It Takes: Characteristics of the Ideal Personal Health Record," Health Aff (Millwood), vol. 28(2), pp. 369-376.

[15] M. Li, S. Yu, Y. Zhen, K. Ren, and W. Lou," Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption" IEEE Trans. On parallel and distributed system, vol. 24(1), UT, Mar. 2012, pp.131-143.

[16] S.K. Manda, and B. Hanmanthu, "Privacy Preserving Support for Mobile Health Care using Message Digest," Int. J. of Advanced Research in Computer Science and Software Engineering," vol. 3, Sept. 2013, pp. 197-102.

[17] Y. Ren, R.W.N. Pazzi, and A. Boukerche,"Monitoring Patients via a Secure and Mobile Healthcare System," IEEE Wireless Communications, vol. 17(1), Feb. 2010, pp. 59-65.

[18] Ukil, S. Bandyopadhyay, and A. Pal,"IoT-Privacy: To Be Private or Not To Be Private," IEEE INFOCOM, Toronto ON, Apr. 2014, pp.123-124.

[19] Tajer, S. Kar, H.V. Poor, and S. Cui," Distributed Joint Cyber Attack Detection and State Recovery in Smart Grids," IEEE Int. Conf. on Smart Grid Communications, Brussels, Belgium, Oct. 2011, pp.202-207.

[20] H.D. Nguyen, S. Gutta, and Q. Cheng," An Active Distributed Approach for Cyber Attack Detection," IEEE Conf. on Signals, Systems and Computers, Pacific Grove, CA, Nov. 2010, pp. 1540-1544.

[21] Li, A. Raghunathan, and N. K. Jha, "Hijacking an Insulin Pump: Security Attacks and Defenses for a Diabetes Therapy System," IEEE 13th Int. Conf. on e-health Networking, Applications and Services, Columbia, MO, June 2011, pp. 150-156.

[22] S.G. Miaou, C.M. Hsu, Y.S. Tsai, and H. M. Chao," A Secure Data Hiding Technique with Heterogeneous Data-Combining Capability or Electronic Patient Records," Proc. of the 22nd Annual EMBS Int. Conf., vol. 1, Chicago IL, July 2000, pp. 280-283.

[23] Slamanig, and C. Stingle," Privacy Aspects of eHealth," IEEE 3rd Int. Conf. on Availability, Reliability and Security, Barcelona, Mar. 2008, pp. 1226-1233.

[24] R. Hall, A. Rinaldo, and L. Wasserman," Differential Privacy for Functions and Functional Data," J. of Machine Learning Research, 2013, pp.703-727.

[25] J. Ren, Y. Li, and T. Li ," Routing-Based Source-Location Privacy in Wireless Sensor Networks," IEEE Int. Conf. on Communications, Dresden, June 2009, pp.1-5.

[26] Y. Jian, S. Chen, Z. Zhang, and L. Zhang," Protecting Recevier-Location Privacy in Wireless Sensor Networks," IEEE 26th Int. Conf. on Computer Communications, Anchorage, AK, May 2007, pp.1955-1963.

[27] K. Mehta, D. Liu, and M. Wright," Location Privacy in Sensor Networks Against a Global Eavesdropper," IEEE Int. Conf. on Network Protocols, Beijing, Oct. 2007, pp. 314-323.