Strengthening Patient's Privacy in IoT Centred Ubiquitous Healthcare Supervision in the United Kingdom

Murtaza Hussain Shaikh¹⁾, Ivevel S. Karlson²⁾, Jongho Kim³⁾

Abstract

The notion of the Internet of Things takes labelled by a grouping of names, mainly comprising on automaton to automaton (M2M), sensor grids, hyper-pervasive computing and smart ubiquitous enumeration. Singularities of improved Internet of Things in healthcare supervision systems include a patient to be recognized assigning an RFID chip has also expanded the peril to the information and essential materials. This paper plugs over the patient partiality based privacy solidification set-up for the Internet of Things centred on the ubiquitous healthcare management system (HCMS), famously known generally for the United Kingdom and Northern Ireland 's healthcare domain. To pledge a British patient's confidentiality to his information, especially in this article the study has tried to describe some real settings and practical stints, which if implemented would decline the risk of data mugging in the hospital information system. The research demographics of this study is the public hospital (Queen Mary's hospital) in London, United Kingdom. For that reason according to the demographic settings, this article familiarizes some advanced methodologies, which are implemented in a diverse automated system, and have been employed into Internet of Things based healthcare supervision system.

Keywords : Internet of Things (IoT), Healthcare, Radio Frequency Identification, Healthcare, Supervision

1. Primer of Healthcare Supervision in the United Kingdom

The upcoming era will be the association between the physical things, the web, and an extensive IoT-based supervision system. The things or objects include merchandise, apparatus, and device. The explanation overdue integrating health care with the Internet of Things highlights into medicinal devices enhances the quality and adequacy of administration, bringing unusually high incentive for elderly citizen and out-patients with chronic conditions and those

Received(August 22, 2018), Review Result(1st: September 11, 2018, 2nd: October 19, 2018), Accepted(December 10, 2018)

1) (Assistant Professor) 48434 Department of Business Administration, Kyungsoong Univ., 309 Suyeong-ro, Nam-gu, Busan, Korea

2) (Professor) Department of Computer Science, University of Bristol, United Kingdom
email: I.S.Karlson @bristol.ac.kr

3) (Professor, Corresponding Author) 48434 Department of Business Administration, Kyungsoong Univ., 309 Suyeong-ro, Nam-gu, Busan, Korea
email: jonghokim@ks.ac.kr

that require constant steady management in the hospitals. This phenomenon as we call the improved IoT (Internet of Things), comprises of all Internet (either online and offline) supported by synchronized objects and the systematized web 3.0 process that permits the secure correspondence and collaboration with those synchronized objects[1]. Now, the advance medicinal science has eternally lingered one of the sizzling application of the Internet world. The alliance of Internet and advance medical discipline molded a sub research area known as e-health, which is well-defined within UK perimeter as *"A smart app of Internet and other related technologies in healthcare administration industry to improve the access, efficiency, effectiveness, quality of clinical and commercial processes exploited by healthcare organizations, stakeholders, practitioners and out-patients in an effort to improve the health status of patients within United Kingdom"*[2].

[Fig. 1] The Core Element and Relationship in an IoT based Healthcare

Along with many other services, nowadays the vital time saving online appointment services, in particular, are thorough communal e-health provisions[3][4]. The e-health provisions is a minor section of Internet of Things positioned healthcare, in which an secured online communication of an out-patient with a senior specialist is through likely beside with open admittance to an online medicinal record examine for the patients. Although IoT based smart health care structure comprises all these favourable credentials of patients, staff, and doctors' sites, following of patient's medicinal records and trailing localities of hospital tools. [Fig. 1] determines the fundamental bond between the three main actors in primary health care supervision.

Truly, an IoT has likewise enabled the intelligent behavior of some apparatus which alarms instinctively, when close to expiration or auto notifying an appropriate senior doctor if his/her

concerned out-patient is admitted, into intensive care unit (ICU) in Queen Mary's hospital. On a note (i.e. this kind of technological practice at present is already available at Queen Mary's hospital, London, UK and is research locale of this study). In such outline, where a local out-patient is assisted with recent technologies, frequent hazard aspects also ascend to his/her delicate information and fitness concerns, which have develop the fragment of the hospital databank administration classification[5]. Further on, in this research work, it has argued in such cases; the third half encompasses of methodologies, which have used to communicate and protect information. Last of all, describes safety perils, which affect healthcare system and contains the resolutions to such peril features like current elucidations and impending debate.

2. Background Realities

It has debated systematically round the shield of patient's confidentiality in e-health facilities, plumbed on numerous 3.0 version of Internet webs, which generate an relations between a British patient and general practitioner of Queen Mary's hospital and clinched some fallouts established on privacy shield of British patients information[3]. They established that *"a privacy and confidentiality are key concerns in e-health services. HIPAA regulations, e-health code of ethics, HON (Health on the Net) principles, and other useful strategies do not ensure that privacy and record protection is properly implied. There is a breach flanked by more attention to the spirit of existing measures and procedures is needed to safeguard patients and privacy privileges"*[6]. It planned an architecture termed MedSN scheme, especially aimed at United States demographics for in-homebased patient observing based on the wireless sensor system and has deliberated it's security apprehensions[7]. Concerning out-patient's medicinal data security, the formation and hastening of data should be optimized and minimized. Privacy inherently shall be measured with endwise, numerous consumers in diverse characters obligation be reinforced, and each with different controls and circumstantial privacy for actors and network information concealment must be well-preserved[8]. In [4] the author has extremely projected the idea of large-scale patients remote checking based on wireless body sensor network (WSN) concepts and suggests seemly cryptographic schemes for privacy preserving.

The prime safety goals of endorsed pattern is privacy. When privacy is fretful inside the application encompasses anonymity, un-linkability, and location privacy requirements. There are two type of Anonymity; medicinal record anonymity and authentication anonymity[9]. The medicinal record anonymity is decreed when recognizing particulars (example, DoB, name,

social security no, telephone no and address) in medicinal database must be concealed from certain parties. Apart from this conversation, the necessary foundation of any medicinal data system consists of main entities as defined in [Fig. 2].

These parties comprise healthcare insurance companies, local administration workforce and any related employees that have no suitable admittance rights. Subsequently, these parties doesn't intricate in a specific setting. Ruminating medicinal information anonymity will not be the prominence of this research study (i.e. the scope of ruminating the clinical data is long and doesn't matches with the theme of this research). Up until now, medicinal record anonymity should be assured, to accomplish a un-linkability. *"Authentication anonymity warrants that patient shall not be recognized when validating to the distant server for medicinal specifics storage in our scenario."*

[Fig. 2] Diverse Objectives in Medical Information System on IoT

It should be prominent that the uniqueness of a patient can be presumed from the Internet protocol address of a smart PDA that communicates the medicinal record over wireless nets if the protocol address of the smart PDA is identifiable. This exposure is connected with employment of (WSN) wireless sensor system'[4]

3. Practical Traits of IoT's Healthcare Scheme

The IoT centered healthcare supervision scheme resides identifiable objects comprising senior doctors and patient's along with medicinal records and tools. In this artefact, the practical

features defined are concerned with privacy guard of a patient's info and allied imperatives to access by the true individuals. To go in more depths, the study have rifted the patient specifics into three (03) sections;

1. Systematic Specifics: Example patients' age, sex, body temperature, BP, blood group, which is not quite profound to unrelated operators, and can be comprehended and retrieved by an individual[6][10]. This specifics could feed by a general duty doctor or a practical workforce inside Queen Mary's hospital.

2. Private Specifics: Just like some severe syndromes, sexual disorder, and DNA samples. Preferably this specifics must be move in by the specialist in the Queen Mary's hospital. However, comprehensive mechanism over the right of entry acquiescence need to be approved by the patient[6].

3. Limited Specifics: It's the specifics in which a patient would like to be part in an exclusive way among a restricted circle of trusted actors, with a promise that a nonentity can have admittance to the specifics[6].

The determination of dividing specifics into such modules is vibrant. A general duty doctor requisite know some chastised evidence like age, patient's sex, blood pressure, but not all the information, whereas a specialist requisite be learned of the proper health situation of the patient to analyze and cure the disease precisely, but that also with the endorsement of patient[10]. In the meantime, the main apprehension in the scheme is the privacy fortification, so we converse here about patient's privacy anxieties (i.e. anonymity, un-linkability, un-observability and location privacy requirements). The authors of this article has elaborate on these privacy concerns simultaneously. An anonymity is a state of not being recognizable. Some patient's want specialist advice deprived of being recognized their names, age and other prime data[3][11]. They might reveal susceptible specifics like severe syndrome deprived of revealing their individuality. Anonymity detached from an organization perception when categorizing the specifics alike (names, age and social security no. etc.) in the medicinal record must hide from certain un-focal entities. These entities contain (e.g. life insurance companies, survey organizations, researchers, some administration staff) that have no proper access rights[9]. Furthermore, Un-linkability means the medicinal record anonymity must assure to attain un-linkability. This is imaginable when pragmatic to such settings in which the patient's particulars is stored on a local computer server, and even if some unauthorized entity get access to use to that delicate particulars, he or she gets pseudo-coded specifics, such that one information he or she gets has no relation to other and therefore making no any sense[4][10]. Also, Un-observability ensures that an actor may utilize a source or facility deprived of others,

particularly 3rd parties, having the capacity to witness that the resources or services are pushed off. This comprises that users' cannot conclude whether an action is actually completed[5]. Last but not least is the location or site; it is an obligation that the location privacy needs to be assured in a distant care situation, where the Internet of Things founded on health supervision coordination is set-up to observe a British patient could be subjected to trail location[7].

4. Privacy & Security Risks

The Royal Medical Association of United Kingdom and Northern Ireland (RMA) issued an exclusive report in the year 2015 on RFID chips implanted in a human, which concluded that "these tiny embedded chips may support to increase the safety and competence for a British patient's comfort"[3]. The RMA highly recommends that, during the process for RFID chip implantation, patients should be well-versed in medicinal uncertainties allied or complications with those smart devices. Though, the health policymakers in the government and doctors in the UK must comprehend that smart radio ID chips, distinct supplementary forms of related medicinal expertise, have a serious impression upon patient's confidentiality that encompasses distant yonder the medicinal domain. With an embedded RFID system, entities can be traced by anybody consuming a generic radio ID chip. "The assent procedure requests to present this peril clearly, and the RMA should modify its report to precisely address this unfamiliar perils"[11]. Patient's subjective data is indispensable in the sense that if it retrieved by unrelated individuals can have a wrong imprint on an acquaintanceship of patient and if altered can crop lethal magnitudes for the patient. So the privacy peril twitches from a very first general duty doctor who assembles prime specifics and allocates a specialist doctor in the UK hospital. The doctor has exclusively reliable an individual who can typically turn on the patient's behalf for several procedures linking the reticent medicinal record[4][10]. An IoT based secure flow down structure determines the peril feature for patient's personal record start from individuals directly associated to him or her, like a primary surgeon, consultant or sometimes an expert, who collects the primary record and process that to the computer system, as the following [Fig. 3] elucidates the risk down strategy.

[Fig. 3] IoT based Secure Flow Down Structure

Another peril aspect is a way general doctor or a computer expert stores specifics to a consistent foundation like the server of healthcare administration in the UK hospital. In the meantime, everything including patient himself his history record are identifiable in an IoT system, so the entire system must be secure enough to protect patient's medicinal information and not accessible nearby remote machines of another IoT based system[7]. Its corresponding actor or user can read the RFID chips, devoted to a patient and his medicinal history record file, but if it is open by an additional reader of the identical configuration, generates significant amounts of peril features, which can root the information mugging and used in a way to mischief the patient's prosperity or his life[9].

5. Proposed Elucidations

Some elementary moralities offered by the United States MedSN system for healthcare, which if dawdled can highly pledge a secure and smooth connection of information between consultant doctors and patients in the hospital setting. The initial elementary morality is the propagation of data should be minimized, and there should be active a privacy measure as end to end. The second elementary morality is multi-actors in unique roles should be livelihood and each with unlike confidentiality concerns[12]. The third elementary morality is contextual concealment for the users/actors and network security must be conserved[13]. Subsequently, the Internet of Things has by now absorbed in many modern technologies, so information examination is not only limited to the healthcare area. Another simple morality is role-based access control. An access proclamation is centred on the roles that discrete actors have a fragment of an organization. Users take on assigned roles (like a head nurse and a concerned patient inside

the Queen Mary's hospital). The author in [6] and [10] has defined a user role, *"the process of defining roles should be based on a thorough analysis of how an organization activates and should include input from a wide spectrum of users in an organization. Role name groups entree rights and the use of assets is restricted to individuals authorized to assume the associated rôle"*. Considering here the example in a top UK hospital arrangement (i.e. in our case it's Queen Mary's hospital), the part of a senior physician or surgeon can contain operations to accomplish diagnosis, recommend medication, and order research lab examinations; could be imperfect to congregation unspecified hospital info meant for training). Usage of roles to switch entry can be an active malicious of enforcing initiative-detailed security policies, and for restructuring the safety administration procedure[6]. Another basic morality is implementing a digital signature to ensure integrity, authenticity in the health-care specifics. A digital signature is substantial by smearing some scientific function to estimate the memo digest of electronic text, and then encode those result of reckoning with a safe signer's private key[1]. In the same manner, the receivers can authenticate the digital signature with the custom of despatcher's public key in a computer server. Digital signatures employ asymmetric cryptography. In cases, it provides a stratum of validation and security to communications directed through a non-secure channel. If appropriately executed a digital-signature provides the receiver motive to consider the requested dispatcher directed the message[14]. Lastly, by applying encryption and authentication contrivance, somehow it can heal the security issue. It is the procedure of transmuting specifics, using a computer algorithm to mark it illegible to everyone excluding related individuals. The encryption can be cast-off to defend documents such as records on computer systems and other media storage devices[12]. Henceforth, secure authentication contrivances are obligatory for an Internet of Things based healthcare supervision environment to make sure the safety of distributing and receipting data packages of the patient. Surely, authentication is an essential procedure before check connection. Only those patients who have assumed the authentication means are only permissible to reception the Internet of Things based on online health-care resources[5].

6. Conclusion

This research study gave an instance of the processes an ordinary British patient's specifics authorizing through in an Internet of Things centred health care supervision system and the linked perils within the United Kingdom's society. It also undertaken some comprehensive

solutions and recommended more depending on settings. Indeed, actors or users who practice the expertise for health-care stated intentions have the genuine to believe that the private specifics they make available will be reserved close. Likewise, have the factual to be acquainted that sensitive or private information may collect, and select whether they will agree with their private data to be collected and whether they will authorize it to be sector. Nonetheless, non-clinical staff and professionals intricate in providing online health-care amenities may be oblivious of the different standards they must follow to when dealing with electronic health-care users and may need to be instructed about the moral responsibility not to abuse British patient's safety and privacy concerns. In a forthcoming era, the authors intend and wish to conduct further work and research on a detailed security framework to safeguard the patient's private information inside a general hospital like Queen Mary and remote clinics in United Kingdom. Successively, the IoT expertise is a state-of-the-art turf in-flowing such kind of smart systems, so a fresh, enhanced and improved security prototypes would be essential for ensuring and protecting privacy.

References

- [1] K. J. Hannah, M. J. Ball, and M. J. A. Edwards, *Introduction to Nursing Informatics* (2nd edition), Springer, NewYork, USA, (2014)
- [2] J. Marconi, *e-Health: Navigating the internet for health information Healthcare, Advocacy White Paper*. Healthcare Information and Management Systems Society, Italy, (2012)
- [3] Y. Hong, T. B. Patrick and R. Gillis, *Protection of Patient's Privacy and Data Security in e-Health*, International Conference on Bio-Medical Engineering and Informatics, (2015), October 14-16; Nottingham, UK
- [4] J. Sun, X. Zhu, and Y. Fang, *Preserving Privacy in Emergency response based on wireless body sensor networks*, IEEE Globecom Proceedings, (2011), December 5-9; Berlin, Germany
- [5] Institute of Medicine, *Crossing the quality chasm: A new health system for the 21st Century*. Committee on Quality of Healthcare in United States America, National Academy Press, Washington DC, USA, (2015)
- [6] L. H. Aiken, S. P. Clarke, and D. M. Sloane, *Hospital staffing, organisation, and quality of care: Cross-national findings*, International Journal of Quality Health Care, (2002), Vol.14, No.1, pp.5-13.
- [7] P. Kuryloski, *Extended Abstract: MedSN System for In-Home Patient Monitoring: Architecture, Privacy and Security*, Joint Workshop on High Confidence Medical Devices, Software, and Systems, (2009), April 16; USA
- [8] M. Evered and S. Bogeholz, *A Case Study in Access Control Requirements for a Health Information*

System, Australasian Information Security Workshop, **(2010)**, July 5-7; Canberra, Australia

- [9] M. Meingast, T. Roosta, and S. Sastry, Security and Privacy Issues with Health Care Information Technology, Proceedings of the 28th IEEE EMBS Annual International Conference, **(2010)**, August 31-September 3; New York City, USA
- [10] J. Kassirer, Patient, physicians, and the internet, Health Affairs, **(2013)**, Vol.19, No.6, pp.115-123.
- [11] S. Kim and D. S. Ko, Design of Infant Health Condition Check Solution Based on a Wearable Device Attitude Heading Reference System, International Conference on Bio-Science and Bio-Technology (BSBT), **(2015)**, November 25-28; Jeju, South Korea
- [12] C. Rotariu and V. Manta, Wireless System for Remote Monitoring of Oxygen Saturation & Heart Rate, Federated Conference on Computer Science & Information Systems (FedCSIS), **(2012)**, September 9-12; Wroclaw, Poland
- [13] M. Al Ameen, Liu, J., and Kwak, K, Security and privacy issues in wireless sensor networks for healthcare applications, Journal of Medical Systems, London, UK, **(2012)**, Vol.36, No.1, pp.93-101.
- [14] P. Gope and T. Hwang, BSN-Care: A Secure IoT-Based Modern Healthcare System Using Body Sensor Network, IEEE Sensors Journal, USA, **(2016)**, Vol.16, No.5, pp.1368-1376.