Global Scientific JOURNALS

GSJ: Volume 5, Issue с, Jǳyŝ 20нл, Online: ISSN нонл-фмус
www.globalscientificjournal.com

PRIVACY AND SECURITY OF PERSONAL HEALTH INFORMATION IN MOBILE HEALTH (MHEALTH) CARE

Solomon SARPONG

KeyWords
Biometrics, personal health information, privacy-preserving, fingerprint

© GSJ

ABSTRACT

Since the turn of the century there has been the advent of many wearable health monitoring devices. This new trend gained traction as health Service Provider (SP) want to know the health status of their clients in real time. Another reason for this is the fascination of people to monitor their health and daily physical activities. The Personal Health Information (PHI) measured by these devices send information by Bluetooth to Smartphones for onward delivery to the SP. However, it has been observed that there are some security issues (privacy of personal health information, location, etc.) associated with such procedure. Hence, discouraging some persons from using it. In lieu of this, this paper proposes privacy-preserving techniques in mobile health without the use of Smartphones. The absence of Smartphones in this protocol brings to the fore added security and hence privacy of PHI is assured. There is also the authentication of the clients' biometrics before the PHI is sent to the SP. This is to ensure that the PHI sent to the SP is from the right client.

INTRODUCTION

A wearable mobile health device refers to a portable device that can be carried and operated with ease as the user moves from place to place and has Internet and wireless communication technologies [1]. Mobile health (mHealth) according to Mathias, [2] is the medical and public healthcare practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants (PDAs), and other wireless devices. Generally, mHealth involves the use and capitalization on a mobile phone's core utility of voice and short messaging service (SMS) as well as more complex functionalities and applications including general packet radio service (GPRS), third and fourth generation mobile telecommunications (3G and 4G systems), global positioning system (GPS), and Bluetooth technology.

Since the turn of the century, there has been a paradigm shift in the way doctors or medical health providers manage and coordinate the care of patients inside or outside a medical facility. This has come about in part as a result of the advent of wearable health devices. These health devices help the health providers to monitor the health conditions of patients anywhere and anytime. Even though this is not a panacea to visiting the health facility, these technologies can help monitor the health conditions of patients or users of wearable health devices.

Prior to the advent of these wearable health devices, doctors/medical providers got information on their patients only when they visited the health facilities. But with the use of mHealth care devices, data on patients are transmitted to the doctor/caregiver at all times. This goes a long way to enable the doctor know the effectiveness of a given treatment as well as the health condition of the patient in real time. As opposed to the patient visiting to the health facility and providing health information, these devices provide continuous and timely data.

The remoteness of the patient from the health facility implies there are some checks and balances that should be put in place. That is, there is the need to sure that the device is accurate and reliable; the data is reliable and has a direct relation with the patient healthcare plan; the data transmitted should be easy to interpret hence, enable the healthcare provider to have a care plan. If all these are in place, the healthcare provider is able to have a complete picture of the patient's health conditions and facilitate any improvements or modifications to healthcare plan.

MHealth Apps allow patients to take control of their own health by applying healthy living practices [3]. The easy availability of personal health information (PHI) on the mHealth Apps, help people manage their lives and actively participate in their own health care and also help doctors provide point of care resources and aid in managing their practices [4].

The willingness of patients to let medical health providers have access to their health records make the implementation of mHealth increase. According to [5] more than a third of users of wearable health devices in America are willing to send medical data to their doctor over a wireless device. However, [6] observed that, 75% Americans consider the privacy of their health information important or very important. There are concerns from some doctors about the security and privacy of the mHealth services [7]. Hence, data security, access control policy and confidentiality are the main issues that must be addressed in order for mHealth to continue to flourish and deliver safe healthcare benefits. For the continuous use of mHealth facilities, the users should be assured of the security of their PHI and that their PHI will be accurately delivered to a health facility.

As more people (people with chronic health conditions and those who are health conscious) become aware of the benefits of mHealth devices, patronage in it has increased [3]. In spite of all these, the challenges facing the mHealth services include; lack of interoperability of systems, lack of coverage of and access to technologies, limited technological literacy and limited capacity to invest in technology (e.g., small businesses, governments, institutions).

To the best of my knowledge, the mHealth devices in use have these disadvantages: (i). When the device is stolen or worn by another person, it will keep on sending PHI to the health facility or hospital. As a result, this may have effect on the prognosis of the patient. (ii). The use Bluetooth connected to a Smartphone [8-12] has been observed to have some disadvantages. These disadvantages include; (a). The Bluetooth may leak the users' information. (b). the user maybe monitored through the GPS on the Smartphone. Even if the GPS on the Smartphone is off, the user can be monitored through the gyroscope and accelerometer on the Smartphone. (c). in case of an emergency, the battery of the Smartphone might have discharged as the Smartphone is used for other purposes (e.g. SMS, Calls, etc.). In lieu of these, this paper proposes a novel mHealth device that authenticates the biometric data of the user before transmitting the PHI. Hence, if the input biometrics change (when the device is worn by another person) the device will not transmit the PHI. There is no use of a Smartphone to avoid the inherent security issues associated with its usage in mHealth. The rest of the paper has the literature review, system model and architecture and conclusion.

LITERATURE REVIEW

Wearable technology cover a broad field from those focused on healthcare and fitness, to industrial applications, and even entertainment and arts [13]. There are some security and privacy weaknesses that make such wearable devices vulnerable to attacks. Other inherent problems of the wearable technologies include power consumption, communication capacity, design constraints, and security issues. Also, as the wearable technologies are not stand alone devices, they are prone to authentication issues and meet-in-the-middle attacks [14]. Furthermore, these devices offer new opportunities to monitor the activities of the client continuously.

However, it improves efficiency, productivity, service and engagement across industries [6]. These devices collect far broader range of information much more continuously and wider range of uses than that collected in traditional health facility settings. The added advantages of mHealth care applications include; faster searching and availability of relevant information, efficient decision-making and quicker documentation by physicians and medical staff. Patients can remain under constant observation of expert physicians without being physically present at the hospitals or health facilities [15]. Also, wearable technologies have the following characteristics; hands-free, always on, environment-aware, attention-getting, connected, and un-monopolizing. In spite of all these qualities, it makes accessing and processing medical data less time consuming hence, more relevant information are available when making decisions [16].

Reliability and accuracy of the data on patients is another important reason for the proliferation of these wearable devices. Reliability and accuracy of the data is of paramount importance hence there is the need for medical grade data instead of consumer-grade data on patience. The use of medical grade data ensures that, information on patience are taken by the devices and transmitted directly to the medical heath providers through cloud services. As the patient plays no part in the collection of the data, it will be reliable and accurate. The reliability and accuracy of these devices are very important as in America alone, about a hundred thousand patients die every year as a result of broken or faulty healthcare devices [17]. Also, [18] puts the deaths between 250,000 and 440,000 deaths per year.

SYSTEM MODEL

Initiation

In this mobile health protocol, there is no need for the use of a Smartphone. This protocol consists the Service Provider (this entails cloud service, Data Centre and health facility (Doctors and Ambulance)), a trusted authority (does the computations on request by client) that is a partner in the mHealth protocol and the individual clients that will be using the device to monitor their health.

Homomorphic Encryption

In order to facilitate oblivious transfer protocols, homomorphic cryptography will be used. The semantically secure light weight additive homomorphic public-key encryption which is used to secure protocols will be used [19, 20]. In homomorphic encryption, the ciphertext can be operated on mathematically without altering the nature of the encryption [21]. Hence in homomorphic encryption, cryptosystem operations can be performed on encrypted information without the private key being known [22, 23]. Assume a client has public and private keys p_k and s_k respectively. A scheme is homomorphic encryption, if there exists a message $m \leftarrow \{m_1, m_2\}$; $E_{p_k}[m_1]$ and $E_{p_k}[m_2]$ can be computed from $E_{p_k}[m_1 \times m_2]$ without knowing p_k. Further reading on homomorphic encryption can be found in, [21- 24].

System Architecture

As a result of the sensitivity and importance of PHIs, the registration, initializing and control of the healthcare system is managed by trustworthy person(s). A client who wishes to use the mobile healthcare system for monitoring his/her health, registers him/her self as a medical user. A medical professional examines the client and generates his health profile. After the generation of the health profile, the client is placed under particular medical professional(s).

© GSJ

Registration is done by a trusted personnel who records the gender, age, emails, the address, telephone number etc. of the client who is then issued an identification tag. The trusted personnel then uploads these information securely to the cloud service. The client uses the identification tag to configure the device on the first usage. For the first time usage of the device, the client generates a password (private key), fingerprints the device and inputs the identification tag.

The password (private key), is exponentiated by the device using the public key of the SP to create a corresponding public key. The device encrypts the public key, the fingerprint and the tag using the public key of the service provider. The device will be measuring and monitoring the health of the client wherever s/he goes. The device is SIM enabled and embedded with location awareness services. The device records the PHI of the client when worn. As part of the registration, the client fingerprints on the device (the device is fingerprint enabled). The fingerprinting prevents the device from unauthorized usage.

The device records PHI of the client in addition to date and time. If the client forgets to fingerprint on the device for the PHI to be sent to the SP, the device notifies the client (by vibrating or sound). When the device is finger printed, the PHI is homomorphically encrypted and sent to the SP. The homomorphically encrypted PHI together with the date and time of the day are encrypted using the public key of the SP and sent to the SP. The SP on receiving this, decrypts and stores it in the data centre. Hence, in the storage, the PHI is homomorphically encrypted but the date and time are not. This is to facilitate data retrieval upon request by the client.

As observed by [25] in normal remote monitoring, the PHI of a patient should be transmitted automatically to a healthcare facility or doctor every 5 minutes. But in this protocol, the patient will be notified (vibration/sound) to be finger printed for information to be sent to healthcare facility. This prevents the PHI of different persons from being sent to the SP in case the device is worn by a different person when misplaced or lost. When the client forgets to fingerprint the device, s/he is notified by vibrating or sound. However, when the device observes extreme measurements (in the case of emergency) the device transmits distress messages including the location to the SP. It has been observed that, ambulance services takes about 8 – 25 minutes for it to arrive in case of an emergency [26-28]. Within this time, by-standers can give only physical help.

When the client needs some information on his/her PHI, the request is made to the SP. The trusted authority homomorphically computes the request and sends it to the client. When the client receives the output of the request, s/he inputs the password created (private key) to see the response to the request. Unlike the mHealth device that uses Smartphones, the device in this protocol deletes the output of the request after a while. This is to prevent the information from being compromised.

EMERGENCY

Unlike what happens in opportunistic mHealth and other existing mHealth systems [8, 29, 30, 31, 9, 10, 11, 12] in case of an emergency, other persons using the same health care system can help. But in this system, in case of an emergency by-standers (even if they are also registered with the same Service Provider) can give only physical help. This is to prevent the leakage of PHI between the person giving the help and the one being helped. With the use of the location awareness service in the device, the client will be located by the ambulance service. There is no usage of a Smartphone in this mHealth protocol because; i). Smartphones are used for other purposes such as phone calls, WhatsApp, facebook, SMS etc. hence the batteries are likely to be low in the cases of emergencies, ii). The configuration of the Apps on Smartphones can allow private PHI to be leaked.

ADVANTAGES

In case the device is stolen or lost, the PHI of the new user will not be sent to the SP. This device will suspend data collection, personal notifications, and access to personal data when the biometrics of the wearer changes, [32]. The PHI is sent to the SP only when the client finger prints the device. As the fingerprint of the new user was not what was used for the registration, the recorded PHI will not be sent to the SP. This protocol has these added advantages as it is not connected to the SP through Smartphone; i). As the health device communicates with the Smartphone through Bluetooth, there is the tendency of leakage of PHI through the Bluetooth; ii). In Smartphones even if the GPS is turned off, the in-built gyroscope and accelerometers measures the users' movement patterns. This hence leaks the Users' location affecting the privacy; iii). The architecture of some of the APPs on the Smartphones also raises privacy issues.

SECURITY

Strong authentication is a critical element to be considered in mHealth care. The authentication ensures that: i). the PHI sent to the SP are associated with the actual client; ii). only authorized individuals have access to data and tools; iii). only valid and protected devices are used and iv). The PHI are sent through authorized channels. In order to ensure adequate security in this protocol the finger print was used. [33, 34] are of the view that, security based on what an individual has (biometrics such as fingerprints and iris patterns) offers a better method of identification and security. The overall goal of effective security protocols is to protect participants' identity and secure data in such a way that if unauthorized individuals gain access to the data, they would be unable to link the data with a particular person or with other data being sent, [35]. The protocol in this paper took into consideration all these security and privacy issues.

CONCLUSION

To make mHealth secure and privacy-preserving of clients' PHI, the protocol in this paper has been proposed. In order to ensure the provision of quality service to the client, only the PHI from the registered client is sent to the SP. This is made possible with the use of the clients' biometrics. It can be stated with certainty that, when the protocol in this paper is implemented, more persons will use mHealth services as the SP will be able to provide secured, privacy-preserving and accurate health care to the clients.

© GSJ

REFERENCES

[1] Shieh Y, Tsai F, Anavim A, Shieh M, Lin M., (2008). Mobile healthcare opportunities and challenges. International Journal of Electronic Healthcare, 4 (2), 208-219.

[2] Mathias L. (). Geo-information: Technologies, Applications and the Environment. Geotechnologies and the Environment, pp. 23 -33.

[3] Varshney, U. (2011) Pervasive healthcare computing: EMR/EHR, wireless and health monitoring, Springer, New York.

[4] Pratt, W., Unruh, K., Civan, A., and Skeels M., (2006) Personal health information management, Communications of the ACM, 49, 1, 51-55.

[5] Cerrato, P. (2011) Mobile medical apps meet the FDA, Part 2, Information Week (available http://www.informationweek.com/healthcare/mobile-wireless/mobile-medical-apps-meet-the-fda-part-2/231901916).

[6] Ponemon L., (2010) Institute, Americans' Opinions on Healthcare Privacy. Available: http://tinyurl.com/4atsdlj.

[7] Pricewater House Coopers B.V. (2014). Consumer intelligence series - The wearable future. https://www.pwc.se/sv/media/assets/consumer-intelligence-series-thewearable-future.pdf.

[8] R. Lu, X. Lin and X. Shen (2013), SPOC: A Secure and Privacy-Preserving Opportunistic Computing Framework for Mobile-Healthcare Emergency. IEEE Transactions on Parallel and Distributed Systems 24(3):614-624, DOI: 10.1109/TPDS.2012.146

[9] Batista M. A. and Gaglani S. M. (2003). The Future of Smartphones in Health Care, AMA Journal of Ethics **(**Illuminating the Art of Medicine**)**, *Virtual Mentor*, 15(11):947-950. DOI: 10.1001/virtualmentor.2013.15.11.stas1-1311

[10] Lippman H., (2013). How apps are changing family medicine. *Journal of Family Practice*, 62(7):362-367. http://www.jfponline.com/home/article/how-apps-are-changing-family-medicine/f8b317bc104214c97c499715fc79cc91.html. Accessed March 15, 2020.

[11] Redelmeier D. A, and Detsky A. S., (2013). Pitfalls with smartphones in medicine. *J Gen Intern Med*.

[12] Lau J. K, Lowres N., Neubeck L, Brieger D. B., Sy R. W., Galloway C. D., Albert D. E., Freedman S. B., (2013). iPhone ECG application for community screening to detect silent atrial fibrillation: a novel technology to prevent stroke. *International Journal of Cardiology*, 165(1):193-194.

[13] Transparency Market Research. (05 Jun, 2014). Wearable Technology Market Research Report 2018. (cited 21 Sep, 2015). [Online] Available: http://www.transparencymarketresearch.com/article/wearable-technology-market.htm

[14] Ching K. W. and Singh M. M., (2016). Wearable technology devices security and privacy vulnerability analysis. International Journal

of Network Security & Its Applications (IJNSA), 8(3), DOI: 10.5121/ijnsa.2016.8302 19.

[15] Bhutkar G., Karande J. B., and Dhore M., (2009). Major Challenges with mobile healthcare applications. Mobile technology, www.bjhcim.co.uk/features/2009/909004.htm

[16] Afrin L. and Daniels M. (2001). PalMER: PalmOS-based access to the enterprise clinical data repository and clinical documentation assistant. AMIA Inc., 848.

[17] Grossman J., (2007). Disruptive innovation in healthcare: challenges for engineering. NAE Annual Meeting Technical Symposium.

[18] Sipherd (2018), The third-leading cause of death in US most doctors don't want you to know about. Modern Medicine. https://www.cnbc.com/2018/02/22/medical-errors-third-leading-cause-of-death-in-america.html (Accessed: 31/03/2020)

[19] Barni M., Failla P., Kolesnikov V., Lazzeretti R., Sadeghi A., and Schneider T., (2009). Secure evalution of private linear branching programs with medical operations. Computer security-ESORICS, pp. 424 – 439.

[20] Yao A. C-C., (1986). How to generate and exchange secrets (extended abstract), Proc., IEEE FOCS, pp. 162 – 167.

[21] Parmar P. V., Padhar S. B., Patel S. N., Bhatt N. I., and Jhaveri R. H., (2014). Survey of Various Homomorphic Encryption Algorithms and Schemes. International Journal of Computer Applications 91(8).

[22] Tebaa, M., El hajji, S., and El Ghazi A., (2012). Homomorphic Encryption Applied to the Cloud Computing Security. Proceedings of the World Congress on Engineering.

[23] El Makkaoi K., Ezzati A., Beni-Hssane A. and Motamed C., (2016). Data Confidentiality in the World of Cloud. Journal of Theoretical and Applied Information Technology 84(3).

[24] Barthelemy L., (2016). A Brief Survey of Fully Homomorphic Encryption, Computing on Encrypted Data. Accessed February 10, 2020. http://blog.quarkslab.com/abrief-survey-of-fully-homomorphic-encryptioncomputing-on-encrypted-data.html.

[25] Yuce M. R., Ng S. W P., Myo L. N., Khan Y. J. and Liu W., (2007). Wireless Body Sensor Network Using Medical Implant Band. *Journal of Medical Systems* volume 31, pp. 467–474, https://doi.org/10.1007/s10916-007-9086-8.

[26] Seow E. and Lim E., (1993). Ambulance response time to emergency departments. Singapore Medical Journal, 1993, Dec., 34(6), pp. 530 – 532.

[27] Steen-Hansen JE and Folkestad EH (2001). How long does it take for an ambulance to arrive? Tidsskr Nor Laegeforen, 121(8); pp. 904 – 911.

[28] Andrew M. S., (2017). Be prepared for ambulance wait times. Health News (Reuters Health), (www.reuters.com/article/us-health-emergency-response-time).

[29] Ambika S., Hamsa P. M., Lalitha R., and Rajakuamri K., (2015). International Journal for Innovative Research in Science & Technology (IJIRST), 1(11), pp. 72 – 77.

[30] Khodankar P. and Talmale R. B. (2016). An attribute based cryptography mechanism for minimum disclosure of sensitive patient health information at emergency mhealthcare. International Research Journal of Engineering and Technology (IRJET), 3(4), pp. 830 - 832

[31] Veeranna B and Gouthami V., (2014). ESPOC: Framework for mhealth emergency. International Journal of Computer Science and Mobile Computing 3(10), pp. 408 – 413.

[32] Kotz D., Carl A. Gunter, Santosh Kumar, and Jonathan P., (2016). Weiner. Privacy and Security in Mobile Health: A Research Agend Computer (Long Beach Calif). 2016 June; 49(6): 22–30. doi:10.1109/MC.2016.185.

[33] Pankanti, S., Bolle, R. M. and Jain, A. (2000) Biometrics: the future of identification. IEEE Computer Magazine, 33(2), 46–49.

[34] Neign, M., Chmielewski, T. A., Jr., Salganicoff, M., Camus, T. A., Seelen, U. M. C.V., Venetianer, P. L. and Zhang, G. G. (2000). An iris biometric system for public and personal use. IEEE Computer Magazine, 33(2), 70–75.

[35] Arora S., Yttri J., and Nilsen W. (2014). Privacy and Security in Mobile Health (mHealth) Research.

© GSJ