Volume: 14 Issue: 01 Pages: 5271-5276(2022) ISSN: 0975-0290

Privacy Risks and Security Threat Strategy to Optimize the Vulnerability in Health Information System (HIS)

Mohammad Amanul Islam
Department of Computer Science and Technology, Xidian University, Xi'an, Shaanxi, China.
Email: aman.cse.bd@gmail.com

ABSTRACT

Health information systems (HIS) generally access, process, or maintain large volumes of sensitive data corresponding to the patient, health service provider (HSP), clinicians, and other stakeholders. Hence, ensuring health data security is a primary concern to improve patient outcomes, inform research, and influence policy-making. Many countries across the world practice data protection and privacy preservation laws against numerous threats related to health data and its communication between the computer networks. Hence, resolving the health information security flaws by designing a potential threat model is always given significant importance. The main objective of this study is to emphasize the concerns related to privacy risks and security threats with the use of HIS.

Keywords – **Exchange, health, information, privacy, vulnerability.**

Date of Submission: Apr 12, 2022 Date of Acceptance: May 26, 2022

I. INTRODUCTION

The proliferation of recent technological advancements and exceptional range of mobile technology usage in the area of healthcare has already been created excessive attention to the demand for health information systems and led to the emergence of a new field called mHealth (Mobile Health). mHealth is a subset of eHealth (Electronic Health) that involves the use of the mobile platform is defined as "The medical and public health practice carried out with mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants (PDAs), and other wireless devices" [7]. mHealth proposes to deliver healthcare applications anytime, anywhere at low and affordable costs [6]. The three key components in mHealth are mobile devices, software platforms (providing basic services such as networking and database), and mHealth applications (apps) [5]. mHealth apps are software applications that can be installed and run on the hardware platform, to help manage chronic diseases, empower the elderly and expectant mothers, remind people to take timely medication etc.

Healthcare involves privacy issues concerning patients, physicians, and primary care providers. The most important aim is to secure:

- Healthcare Information Systems
- Prevent unauthorized people from accessing medical records and confidential information [4].

Health information exchange (HIE) involves the patient's sensitive health data being exchanged through wireless networks and thus addressing the privacy and security concerns in the usage of mHealth [31] apps is essential. It has been reported that more than 500,000 new malware variants surface regularly [3] in networked interconnectivity at present. Many apps provide extensive clauses regarding data collection included in privacy policies. Users are presented with options to select their willingness to share data but most of them are surprised by the amount of data leakage that takes place via their phones [1, 2]. Most users are not fully aware of what data is being collected and how it is used or reused [8].

II. PRIVACY AND SECURITY

In the IT domain [9, 10, 11, 31] information security and data privacy obstruct the adoption or diffusion of technology. Privacy are more directed towards the appropriateness of technology to safeguard personal information. mHealth apps stores communicate personal information about users, and this unfamiliarity with the app environment develops many app-related privacy concerns for consumers. mHealth has empowered users to manage their own health creating a shift from the physician's office to mobile apps and storage in the cloud [12] which raises many privacy and security concerns [13]. According to National Committee on Vital and Health Statistics [14], "Health information privacy is an individual's right to control the acquisition, uses, or disclosures of his or her identifiable health data. Confidentiality refers to the obligations of those who receive information to respect the privacy interests of those to whom the data relate. Security refers to physical, technological, or administrative safeguards or tools used to protect identifiable health data from unwarranted access or disclosure [14]. The following research questions in the Table I have been formulated to turn our focus on the

Volume: 14 Issue: 01 Pages: 5271-5276(2022) ISSN: 0975-0290

issues interrelated to health data security threats and privacy risks:

TABLE I. RESEARCH QUESTIONS AND METHODOLOGIES

	Research Question (RQ)	*Motivation*	*Methodology*
RQ1.	What are the general privacy and security concerns underlying the use of mHealth apps?	This question allows us to get an overview on different privacy and security issues prevalent in mHealth apps usage and what measures can be taken to avert them.	By reviewing the previous work.
RQ2.	what are the measures that can be used to address privacy risks and security issues?	This question permits us to study the privacy risk and security features available in the mHealth apps.	By reviewing the previous work.
RQ3.	What to define a HIS threat model HIS to resolve security flaws?	This question drives us to study the vulnerable areas of system infrastructure.	By illustrating a designed system and identifying the security gaps in previous work.
RQ4.	What kind of operation and maintenance policy TEC service should follow to avoid cyberattacks on HIS?	This question allowed us to comprehend the regular IT practices that can follow for the safe use of mHealth app.	By studying the IT risks and audit trails as standard policy practice documentation in previous work.

III. PRIVACY RISKS

RQ1: In order to address the first research question, privacy risks and security facts in mHealth apps have been identified with the help of an extensive literature review.

Poor Data Collection and Inappropriate Storage Mechanisms: The ubiquitous data collection of mobile devices poses serious privacy and security concerns. In many cases, this information is used to push notifications and provide supervision. A study that analyzed 600 most frequently used apps, found that only 183 (30.5%) had privacy policies. Two-thirds (66.1%) of privacy policies failed to address the app itself [15]. The available privacy policies were not transparent to the users in terms of their privacy practices, required college-level literacy, and were often not focused on the app. Developers fail to inform users about how their data is being used or excessively demand their data [16].

Disclosure of Information: mHealth apps also pose challenges in attaining user consent regarding the data while it is being exchanged in many cases [17]. Hence, such acts may raise significant security and privacy challenges [18]. Moreover, many non-commercial mHealth apps initiate data sending, connect to third-party advertisers/sites, allow them to store it externally, and use unencrypted connections. Some mobile apps use the internet connection to track and record a patient's condition or activity in real-time with the help of embedded sensors on their phones which can pose a security threat. Access to such data discloses detailed information about the user's habits, location, and movements which further exaggerates the risks. According to a survey conducted on 23 most popular free health apps, it was found that 50% send data to third-party advertisers and 39% send data to unidentified parties without any data encryption of which users have not been informed [19].

IV. SECURITY TREATS

The mHealth apps handle increasingly sensitive data for professionals and patients over unsecured Internet communications and third-party servers. Collected sensitive data can be sniffed, injected or put into system logs where it is not secured. In many cases, unencrypted files are placed into removable disks that can be accessed by any other app. Since, sensitive information can inferred using malicious app, its required to protect the internet, third-party services, bluetooth, logging, removable disk, exported components, and side channels [13] to ensure a secure use of the mHealth app.

Data Encryption: Encryption is defined as the form of converting text into a format that is difficult to understand by an unauthorized user. Without encryption, apps causes the risk of exposing data to any unauthorized use or being hacked, stolen, or displayed in an inappropriate location. This risk is serious if the device has malware or spyware. A study shows that only a few paid apps are encrypted out of 43 commercial health and fitness apps while the user's data is collected by the apps [23].

Device Vulnerability: Losing mobile phones or a lack of security authentication poses higher privacy and security concerns. Research reports that 31% of mobile owners have lost their phone or had it stolen, while 12% of mobile phone owners inform that another person has accessed their phone's contents in a way that made them feel that their privacy had been invaded [22].

Data Security Breaches: The risk of data breaching is the most worrying and impeding aspect of mHealth adoption. At present, many doctors can view patients' records without patients' concern which could further lead to medical identity theft. Data breaches occur when medical records are stored or transmitted from one server to another. Hence, practicing encryption techniques can be used [20] to avoid this risk.

Additionally, identifying network infrastructure vulnerabilities should be in regular security practices in HIS. Following the above task, necessary network security practices [32] such as IDS or IPS implementation, a virtual private network (VPN), VPN tunnel between end-

to-end the stakeholders, secure VPN access to the server for the remote health officials or devices, etc., should be ensured.

However, a patient's clinical data has already been extensively acknowledged as significantly critical to the widespread adoption of mobile technology in the healthcare domain [21]. Therefore, the consequence of a data breach becomes very significant.

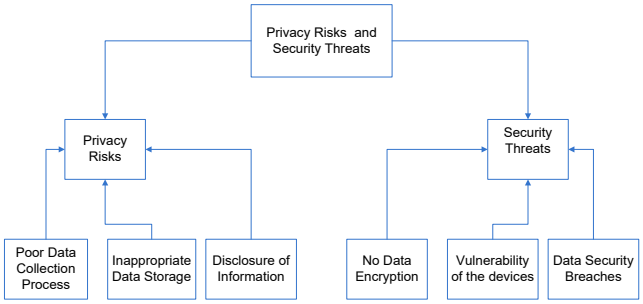

Fig. 1.Privacy and Security Threats in mHealth app usage

V. PRIVACY AND SECURITY MEASURES

RQ2: In order to address second research question, a few HIS privacy risks and security measures have been illustrated by analyzing some major software requirement paradigm, storage data accessibility, data confidentiality and system OS vulnerability.

As recommended in various studies, the following Table II represents the privacy risks and security threats. Additionally, the mentioned measures can be initiated to prevent the vulnerabilities. It also may hinder the adoption of mHealth apps by users.

TABLE II. MEASURES TO AVOID THE PRIVACY RISKS AND SECURITY THREATS

Privacy Risks and Security Threats	*Measures to Initiate Methodology*
Data Collection Procedure [24]	User shall be known about the data is being collected; Educate users about the purpose of the collected data; Provide options to control what data users can share.
Data Storage [13, 25, 26]	Apps to store data on a secure server or in a cloud; Store the sensitive information by encrypting or authenticating it with a username and password.
Data Transmission [25, 28]	Accessing data over an unsecured Wi-Fi network or hotspot should firmly be prohibited.
Data Accessibility [27]	Multi-factor authentication e.g., password, One-time password (OTP) should be enabled to access the mHealth apps.
Data Encryption [24, 26, 28]	End-to-end web request/response shall encrypt the sensitive data in transit via SSL/TLS encryption mechanisms; Sensitive profile data must follow the most industry-practiced encryption algorithm like AEA in 128-bit for both the blocks and keys, WPA2 in 128-bit key etc.
Data Breach [27, 29]	Install firewalls/anti-virus for both the personal computer (PC) operating system (OS) and network IOS to protect against virus/malware-based attacks and malicious applications.

VI. THREAT MODEL

RQ3: To address the third research question, a threat model for a mHealth system has been designed that is composed of some threat components, and the location of each component has been identified for better discovery of privacy risks and security threats.

A. *Threat Model Structure*

In this step, threats shall be plotted to the system architecture design based on all the information collected from the authority [30]. The threat modeling [33] expert will find out the security threat components assets, security controls and threat agents, and also can identify the possible locations for each of them. The application of threat modeling with a simplified system structure has shown in the Figure 2.

B. *Threat Model Components*

In Figure 2, the threat model structure of the system demonstrates the system design with three key components: assets, threat agents, and controls, and thus it helps find out the possible threat and vulnerabilities. However, the threat model also shows the location of each component inside the system architecture.

The assets are the data which are needed to be protected with the highest security. Security controls are the mechanism that must be implemented to ensure reliability. Threat agents are external and internal adversaries who might propose a threat to the system after deployment.

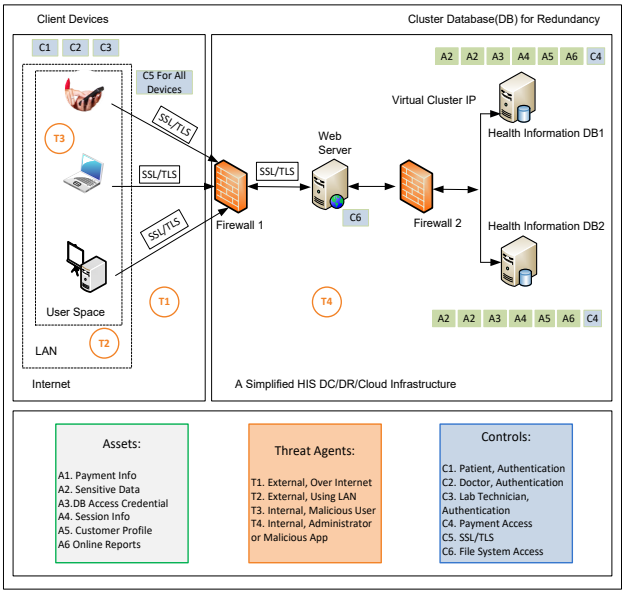

Fig. 2.Threat Model for a Health Information System

Volume: 14 Issue: 01 Pages: 5271-5276(2022) ISSN: 0975-0290

Assets: As we can see from Figure 2, assets are primarily located in the database and data like payment information, database access credentials, session id, patient profile etc. Assets are marked with light green markers in the diagram.

Controls: Controls are located both on the user side and server-side of the system. On the user side, possible controls are the credential authentication of the users and ensuring the use of TLS/SSL that ensures secure communication over the internet. Controls are marked with light blue markers in the diagram.

Threat Agents: Threat agents are of many types. They can be initiated from both external and internal environments. The possible threat initialization points are marked with red markers in the diagram.

It can be assured that a healthcare organization can optimize network security and identify vulnerabilities while protecting the privacy of the users with the help of this threat model.

VII. TESTING AND AUDIT

RQ4: In order to address fourth research question, it is recommend to accomplish a periodical IT risk assessment test and audit.

It can be assured that a healthcare organization can optimize network security and identify vulnerabilities while protecting the privacy of the users with the help of this threat model.

A. Testing

Ensuring privacy through proper use of the technologies is the main goal of testing. It should be exhibited in the period of system development that may include the followings:

i. The designated test verifies that the system ensures strict authentication and authorization control as most of the attacks on systems are done primarily by getting access to associated accounts.
ii. Ensure secured coding by experts during the development period of the system as inferior coding makes the system more vulnerable to the hackers.
iii. A penetration test or simulated cyberattack on the system should be generated to identify vulnerabilities and system flaws before the system launch.

B. Audit

An audit team will do the continuous check-ups routine. The audit team must perform scheduled IT audit periodically and ensure the followings trials:

i. The risk assessment must be performed to analyze upcoming as well as existing risks. Risk assessment reports should be regularly generated and studied.
ii. Collecting information regarding the network and access policies. The information must include:
    a) Log files generated from the firewalls and servers must be collected for analytical study.
    b) A complete list of password failures, lost password cases, and misplaced credentials.
    c) Outdated antivirus incidents must be kept.
iii. Vulnerability analysis must be done on all the information collected by the audit team to get updated about the scale of the existing cyber security flaws in the system.
iv. The audit team should do a regular penetration test. They must generate test reports by prioritizing the vulnerable cases.
v. Another responsibility of the audit team would be to ensure proper knowledge on the user perspective. Audit team may arrange a short training program for the employees on how they should act to protect the users privacy and maintain security in the healthcare organization. They can also send short training videos to employees and users for creating awareness about cyber security.

VIII. CONCLUSION

Adversary attempts on the health information system are susceptible to attacks from a range of numerous legitimate or non-legitimate sources. Hence, our work has demonstrated a threat model over a simplified system infrastructure for the hospitals and healthcare organizations to encounter the threats before appearing it. Additionally, this work has assessed the strategies to secure health information in every step like fitness data collection, storing, exchange, and secure data access. In this era, users are technically able to exercise more control over the security of HIS. Hence, despite developing the policy framework for protecting privacy risks and security threats, continuing further study on allowing secure health information exchange and data integrity is significantly mandated.

REFERENCES

[1] Lin, J., Amini, S., Hong, J. I., Sadeh, N., Lindqvist, J., & Zhang, J. (2012, September). Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. *In Proceedings of the 2012 ACM Conference on Ubiquitous Computing* (pp. 501-510). ACM.

[2] Lederer, S., Mankoff, J., & Dey, A. K. (2003, April). Who wants to know what when? privacy preference determinants in ubiquitous computing. In CHI'03 extended abstracts on Human factors in computing systems (pp. 724-725). ACM.

[3] Emmnauel, U., & Mohammed, T. (2017). Cyber security, threat intelligence: Defending the digital

Volume: 14 Issue: 01 Pages: 5271-5276(2022) ISSN: 0975-0290

platform. Journal of International Technology and Information Management, 26(1), 138-160.

[4] AlHamad, A. Omari, F., & AlHamad, A. (2014). Recommendation for Managing Patients' Privacy in an Integrated Health Information Network, Journal of IT and Economic Development, 5(1), 47-52.

[5] Rebolj, D., Menzel K.,(2004).Mobile computing in construction, ITCon 9, 281–283.

[6] Akter, S., & Ray, P. (2010). mHealth-an ultimate platform to serve the unserved. Yearb Med Inform, 2010, 94-100.

[7] Kay, M., Santos, J., & Takane, M. (2011). mHealth: New horizons for health through mobile technologies. World Health Organization, 64(7), 66-71.

[8] Shklovski, I., Mainwaring, S. D., Skúladóttir, H. H., & Borgthorsson, H. (2014, April). Leakiness and creepiness in app space: Perceptions of privacy and mobile app use. *In Proceedings of the 32nd annual ACM conference on Human factors in computing systems* (pp. 2347-2356). ACM.

[9] Cho, H., Rivera-Sánchez, M., & Lim, S. S. (2009). A multinational study on online privacy: Global concerns and local responses. New Media & Society, 11(3), 395-416. http://dx.doi.org/10.1177/1461444808101618

[10] Zorotheos, A., & Kafeza, E. (2009). Users" perceptions on privacy and their intention to transact online: A study on Greek internet users. Direct Marketing: An International Journal, 3(2), 139-153. http://dx.doi.org/10.1108/17505930910964795

[11] Lee, C. H., Eze, U. C., & Ndubisi, N. (2011). Analyzing key determinants of online repurchase intentions. Asia Pacific Journal of Marketing and Logistics, 23(2), 200-221. http://dx.doi.org/10.1108/13555851111120498

[12] Faruque, M., Mia, M.B., Chowdhury, M.H., Sarker, F., Mamun, K.A. (2019). Feasibility of Digital Health Services for Educating the Community People Regarding Lifestyle Modification Combating Noncommunicable Diseases. In: Streitz, N., Konomi, S. (eds) Distributed, Ambient and Pervasive Interactions. HCII 2019. Lecture Notes in Computer Science, vol 11587. Springer, Cham. https://doi.org/10.1007/978-3-030-21935-2_25

[13] He, D., Naveed, M., Gunter, C. A., & Nahrstedt, K. (2014). Security concerns in Android mHealth apps. *In AMIA Annual Symposium Proceedings* (Vol. 2014, p. 645). American Medical Informatics Association.

[14] Web Ref. Definitions of Privacy and Security: https://www.cdc.gov/nchs/data/ncvhs/ncvhs06-08.pdf Accessed 20th September 2017

[15] Sunyaev, A., Dehling, T., Taylor, P. L., & Mandl, K. D. (2014). Availability and quality of mobile health app privacy policies. Journal of the American Medical Informatics Association, 22(e1), e28-e33.

[16] Ackerman, L. (2013). Mobile health and fitness applications and information privacy. Privacy Rights Clearinghouse, San Diego, CA.

[17] Ranchordas, S., & Kaplan, B. (2016). MHealth for Alzheimer's Disease: Regulation, Consent, and Privacy Concerns.

[18] Faudree, B., & Ford, M. (2013). Security and Privacy in Mobile Health. CIO Journal.

[19] HealthCareBusinessTech. 2014. "Mobile Health Apps Create Privacy Risk, Study Says." Retrieved 27 September - 2017, from http://www.healthcarebusinesstech.com/mobile-health-apps-privacy/

[20] Bhuyan, S. S., Kim, H., Isehunwa, O. O., Kumar, N., Bhatt, J., Wyant, D. K., & Dasgupta, D. (2017). Privacy and security issues in mobile health: Current research and future directions. Health policy and technology, 6(2), 188-191.

[21] Farzandipour, M., Sadoughi, F., Ahmadi, M., & Karimi, I. (2010). Security requirements and solutions in electronic health records: lessons learned from a comparative study. Journal of medical systems, 34(4), 629-642.

[22] Olmstead, K. (2014, April 29). Mobile apps collect information about users, with wide range of permissions. Retrieved from http://www.pewresearch.org/fact-tank/2014/04/29/mobile-apps-collect-information-about-users-with-wide-range-of-permissions/

[23] McCarthy, M. (2013) Experts warn on data security in health and fitness apps. British Medical Journal (f5600), http://www.bmj.com/content/347/bmj.f5600 (accessed 25 February 2017).

[24] Arora, S., Yttri, J., & Nilsen, W. (2014). Privacy and security in mobile health (mHealth) research. Alcohol research: current reviews, 36(1), 143.MEASURES TO AVOID THE PRIVACY AND SECURITY RISKS WHILE USING MHEALTH APPS

[25] PRC, 2016 : https://www.privacyrights.org/printpdf/67502 Accessed 31st march,2018

[26] Jain, A. K., & Shanbhag, D. (2012). Addressing security and privacy risks in mobile applications. IT Professional, 14(5), 28-33.

[27] Adhikari, R., Richards, D., & Scott, K. (2014). Security and privacy issues related to the use of mobile health apps. ACIS.

[28] Addonizio, G. (2017). "The Privacy Risks Surrounding Consumer Health and Fitness Apps, Associated Wearable Devices, and HIPAA's Limitations"

[29] Figg, W.C., Ph.D, and Kam, H.J., M.S. 2011. "Medical Information Security," International journal of Security (IJS) (5:1).

[30] Haque, AKM Bahalul and Pranto, Tahmid Hasan. "Health Data Security: A Privacy-Preserving Proposed Strategy for Bangladesh Health Data Security: A Privacy-Preserving Proposed Strategy for Bangladesh", International Journal of Emerging Technologies in Engineering Research (IJETER), Volume 8, Issue 7, July(2020).

Volume: 14 Issue: 01 Pages: 5271-5276(2022) ISSN: 0975-0290

[31] Sampat, Brinda Hansraj, and Bala Prabhakar. "Privacy risks and security threats in mHealth apps." Journal of International Technology and Information Management 26.4 (2017): 126-153.
[32] OLOYEDE A.O., YEKINI N.A., AKINWOLE A.K., OJO O (2021). Firewall Approach to Computer Network Security: Functional Viewpoint. In Int. J. Advanced Networking and Applications. Volume: 13 Issue: 03 Pages: 4993-5000(2021) ISSN: 0975-0290.
[33] Mohammed Suliman, Bandar Alluhaybi (2022). Protecting Mobile Agent against Man-In-The-Middle Attack: The Dummy Agent Model. In Int. J. Advanced Networking and Applications. Volume: 13 Issue: 04 Pages: 5024-5028(2022) ISSN: 0975-0290.

Biographies and Photographs

Mohammad Amanul Islam is now working as a Consultant (System Engineer), National Spatial Data Infrastructure (NSDI), Bangladesh under Survey of Bangladesh (SoB) & JICA. He has completed his PhD degree in Computer Science and Technology from the Xidian University, Xi'an, China. His research interests include computer and network security, applied cryptography. He is also interested to the application of secure computation technology, and data mining techniques to enhance network security and data privacy.