Networking Issues for Security and Privacy in Mobile Health Apps

Yasser Mohammad Al-Sharo
Faculty of Information Technology, Ajloun National University, Ajloun, 26810, Jordan

***Abstract*—It is highly important to give social care on the personal information that is collected by mobile health applications. There has been a rise in the mobile applications which are applied in almost all the departments and this is as a result of the high technological advancement globally. The developers of these applications need to be somehow reluctant in maintaining the privacy of information collected through the applications because many release insecure apps. The aim of this report is to analyze the status of privacy and security in relation to mobile health. The analysis or the review has been done through academic literature review, a study of the laws which regulate mobile health in the EU and USA. Also, lastly, giving a recommendation for the mobile application developers, on how to maintain privacy and security. As a result, other certifications and standards will be proposed for app developers and another guide for the researchers and developers as well.**

Keywords*—Wireless networks; security; privacy; mobile; analyses

I. INTRODUCTION

Wireless networks and mobile communications have been appropriated by the tremendous advancements in informatics and telecommunications [1],[2],[3]. There has also been the advancement of mobile phones and more so smartphones through modern features such as high processing capabilities, high storage, and high network speeds [4]. It was estimated by the end of May 2014 that there were about 7 billion mobile subscriptions and in the year 2013, there were already 1.8 billion units of mobile phones. Additionally, for those units, 1 billion was for smartphone holders which shows the significant progress [5]. The application market is a new part of the software industry that was facilitated by the smartphones. This is a market which is growing at a very high rate. Forexample, Google Android and Apple IOS operating systemsalready have more than 800,000 applications The healthcare industry has taken full advantage of this market and lives have been transformed through mobile health [6][7]. From the number mentioned Google and Apple Operating systems have got 16,000 and 31,000 health care apps, respectively [8][9][10][11]. The medical applications aredefined as public and medical health practices supported by mobile devices or mobile health/mHealth by the World Health Organization [12][13].

In the development and release of apps, for one to berecognized some key aspects have to beproperly considered and among them,there is security and privacy more so for these apps which deal with non-transferrable and personal data. Mobile applications are today storing privates and personal health information and even health status and this data should be for the individuals to use [14][15][16], control, acquisitions and use according to the National Committee for Vital and Health Statistics (NCVHS) of the United States [17]. Confidentiality is supposed to be highly observed and this refers to the obligations as to which will receive certain information so as to maintain the owner's privacy [18][19][20]. On the other hand, security refers to the administrative, technological, physical tools and safeguards that are used in protecting health information from unwarranted disclosure or access [21].

Reliability and mobility have been the growing requirements following the introduction of new technologies such as cloud computing and the internet of things and easy access to mobile devices [22]. However, the internet has not been able to meet the design demands and hence the complexity has jeopardized scalability and performance. Consequently, researchers have looked into ways that the design of the internet can be changed to meet the changing demands. There have been new approaches for internet protocols, mechanisms, and services. Some of the researcher'sproposedsolutions have not taken into account compatibility with current internet and hence it has not Wireless networks and mobile communications have been appropriated by the tremendous advancements in informatics and telecommunications [1],[2][3]. There has also been the advancement of mobile phones and more so smartphones through modern features such as high processing capabilities, high storage, and high network speeds [4]. It was estimated by the end of May 2014 that there were about 7 billion mobile subscriptions and in the year 2013, there were already 1.8 billion units of mobile phones. Additionally, for those units, 1 billion was for smartphone holders which shows the significant progress [9][5] . The application market is a new part of the software industry that was facilitated by the smartphones. This is a market which is growing at a very high rate. For example, Google Android and Apple IOS operating systems already have more than 800,000 applications The healthcare industry has taken full advantage of this market and lives have been transformed through mobile health [6][7]. From the number mentioned Google and Apple Operating systems have got 16,000 and 31,000 healthcare apps, respectively. The medical applications are defined as public and medical health practices supported by mobile devices or mobile health/mHealth by the World Health Organization [23][11].

In the development and release of apps, for one to be recognized some key aspects have to be properly considered and among them, there is security and privacy more so for

these apps which deal with non-transferrable and personal data. Mobile applications are today storing privates and personal health information and even health status and this data should be for the individuals to use control, acquisitions and use according to the National Committee for Vital and Health Statistics (NCVHS) of the United States [24] [25]. Confidentiality is supposed to be highly observed and this refers to the obligations as to which will receive certain information so as to maintain the owner's privacy [26]. On the other hand, security refers to the administrative, technological, physical tools and safeguards that are used in protecting health information from unwarranted disclosure or access [19].

Reliability and mobility have been the growing requirements following the introduction of new technologies such as cloud computing and the internet of things and easy access to mobile devices [1],[3],[27]. However, the internet has not been able to meet the design demands and hence the complexity have jeopardized scalability and performance. Consequently, researchers have looked into ways that the design of the internet can be changed to meet the changing demands. There have been new approaches for internet protocols, mechanisms, and services. Some of the researcher's proposed solutions have not taken into account compatibility with current internet and hence it has not been adopted. It would be good if the proposed architectures were designed from scratch so as to provide better performance and abstraction which will be based on new principles [28]. However, the clean slate approach which is proposed by researchers do not adopt a future internet architecture. It is good that the whole architecture is remodeled so as to take into consideration all the possible aspects. Reliability of the intent new structure needs to be highly addressed and with it, there must be mobility of control, scalability, quality of service, flexibility, and security [29].

There is a dire problem that patients and clinicians have got a high rate of mobile technology adoption compared to the rate that the designers and developers are making the technologies more private and secure. Health Information and Management Systems Society (HIMMS) conducted a survey on mobile technology uses by the clinicians. 93% are said to be using their phones to access EHR while the collect 45% of data at the bedside which is an increase from 30% in the previous year [30],[31]. Most of the medical student and physicians are not usually aware of the security and privacy aspects of the mobile application which they use during their daily activities. It wouldbe good if the proposed architectures were designed from scratch so as to provide better performance and abstraction which will be based on new principles [23][32][25]. However, the clean slate approach which is proposed by researchers do not adopt future internet architecture. It is good that the whole architecture is remodeled so as to take intoconsideration all the possible aspects. Reliability of the intent new structure needs to be highly addressed and with it,there must be mobility of control, scalability, quality of service, flexibility, and security.

There is a dire problem that patients and clinicians have got a high rate of mobile technology adoption compared to the rate that the designers and developers are making the technologies more private and secure. Health Information and Management Systems Society (HIMMS) conducted a survey on mobile technology uses by the clinicians. 93% are said to be using their phones to access EHR while the collect 45% of data at the bedside which is an increase from 30% in the previous year [29][26]. Most of the medical student and physicians are not usually aware of the security and privacy aspects of the mobile application which they use during their daily activities; Fig. 1 shows the components of E-health networking.

Sensitization is needed in this area because the current understanding and knowledge are low [18][16]. Physicians and medical students need to be aware of security and also health institutions which are okay with the Bring-Your-Own-Device (BYOD) approach. The reason for this is that there are potential cost savings and conveniences associated with the approach. Another issue is that cultural and legal differences in the m-health field need to be overcome between nations and regions. In this field, there are the telecommunication and medical devices which are continuously converging. Most of the regulators are challenged when it comes to keeping up with the converging [17][13].

There are some researchers whom in their papers have addressed m-Health privacy and security but they have done in general [33]. There is a few numbers of researchers who have addressed security and privacy laws regarding mobile health. As a result, the aim of this report is to have the current status evaluated and then give guidelines that developers and designer of apps can follow so as to meet the security and privacy need [23],[20]. The authors of the paper will develop a privacy and security laws review on m-health in the already developed countries with much focus on the USA and the EU [21]. Secondly, a systematic review will be developed from the existing bibliography about issues and concerns that have been found entailing security and privacy in m-health applications [26]. Lastly, with the understanding gained from the reviews, recommendations will be given regarding security and privacy so that the different laws' requirements can be fulfilled. Fig. 2 shows the interactive between components with controller device.

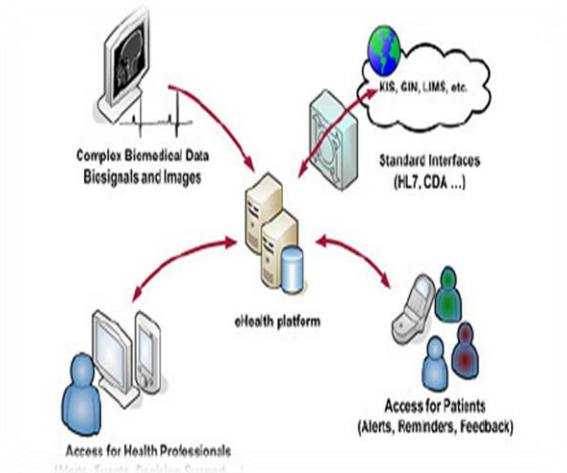

Fig. 1. E-Health Networking.

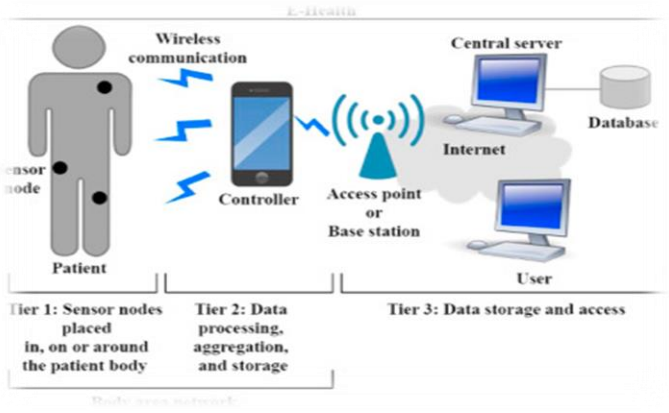

Fig. 2. Body Area Network (Wireless).

II. Research Methodology

The laws from Asian countries have been compared to those of European and American countries because they are different. In the report, the privacy and security laws of the researchershave covered the laws of countries such as Japan and China which are considered by the developers and designers before the development of apps. The United States regions and the EuropeanUnion have been appointed as those zones with high market for mobile apps since they are occidental developed countries [34]. A limitation of the research is that it has considered the legal laws and not frameworks or certifications about privacy and security. The legal laws have been the only once regardedbecause theyform part of the useful frameworks that lead to the issuance of certifications that are critical aspects taken into account by designers. The problem with the mobile apps industry is that there are many individual app developers rather than organization or companies and hence people are not first given the certificates. Part of the study hasalso taken into considerations the ISOIEC 27002/2013 because it is also the foundation of security expert regulations.

However, the huge attention of the authors was given to the m-Health aspects. The first part of the study is that of privacy and security laws review for the mobile health in the United States and the European Union. The procedures which were undertaken in first getting a good understanding of the laws following thorough reading, the main differences,and common aspects are then retrieved from the laws. The last objective is getting together the laws which should be considered by each and every app developer and designer in consideration to the m-Health applications. One researcher or author was in charge of the process for identifying, reading and extracting the key laws. A second author did a further verification during the results revision stage. Any changes which were necessary were made into effect. The part which followed is that of the literature review where a thorough review was done on the security and privacy aspects which are applied when it comes to matters of app development.

The authors of the paperpreferred to seek secondary data from published papers and the databasesystem which were used to source the articles are Explore, IEEE, PubMed, Web of Knowledge and Scopus. The keywords which were used to retrievedata from the articles were: Health and Smartphones, Privacy and Security, Mobile and Health [7],[35], Health and Apps. All the paper types which were used in the search were applied in the study; encryption, Privacy, and Security in apps, system proposals, authentication, privacy reviews,and secure data transfer techniques. Despite the privacy and security terms beingcompletely different, the researchers were using them for two main reasons: one is that the results were limited and the authors had a special interest of the similarities between them. In the determinationofthe articles which could bereviewed, it was those papers published in English and whose date of publication was not more than eight years ago. Therefore they were papers from 2007 to 2014 [22]. Additionally, all the sources must have covered health-related information. The process for paper selection is as shown in Fig. 3.

From a first search from the system, a total of 636 papers were returned. 389 papers were repeated and from the remainingpapers, only 46 were disregarded because they were not addressing the study issues. As a result, a total of 201 papers were used for the study. Since the exclusion and inclusion of the papers depended on the author's opinion, independent verification was done on the papers because it was not all clear from the articles abstracts. The search for the articles was done by one author while the others reviewed the papers. After the determination of the researchmethods, the articles were classified into groups. The results obtained from the articles was what used to draft the recommendation for the security and privacy laws. The researchersalso convened so as to discuss those techniques which should be the most appropriate in fulfilling the studied laws.

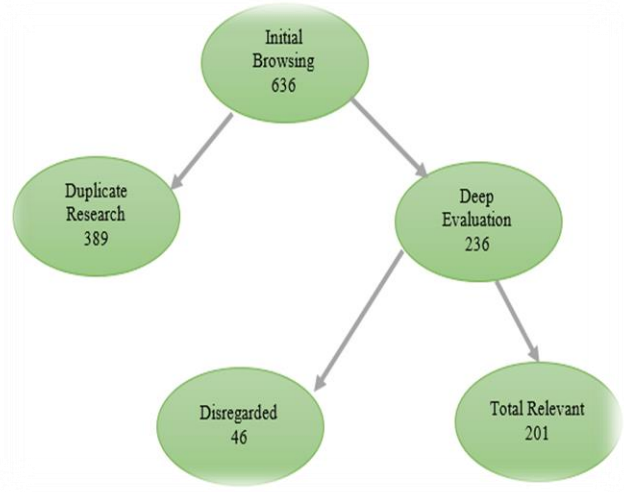

Fig. 3. Flowchart of the Literature Review Steps.

III. RESULTS

From the study of privacy and security laws in the United States and the European Union, it was clear that the European Union has got a law which addresses privacy and security in mobile health. It is more of a general directive that guides member states what they are expected to apply in their laws. It is the European Union Data Protection Directive 95/46/EC structured in the year 1995 [36]. In the year 2012 [37], a draft of the EU Data Protection Regulation was approved When a law is passed by the European Union there is no need to have the member states implement it because it is already enforced [32][38],[39].

Contrary to the European Union, the USA usually provides a number of laws regarding security and privacy in the mobile health. In the United States, the law which applies to mobile health issues has got similar concepts as that of the EU and it is the Health Insurance Portability and Accountability Act(HIPAA) [40]. The law does protect digital health information privacy which is also part of the FTC Act in Section 5. FTC stands for the Federal Trade Commission. The law was also successful in regulating mobile Health privacy aspects in the report. The aspects include "Mobile Privacy Disclosures" where trust is usually built through Transparency. There is also a special law which protects the children under the age of 13.it is called the Children's Online Privacy Protection Act (COPPA) the law was structured in the year 1998. It prevents gathering of information from children without the consent of legal tutors or parents. There are also certain state laws but their content was not considered in the study [41][42]. A law restrictiveness is based on the mentioned laws points compared to others based on common requirements of the information.

The summary of restrictive points in all the mentioned laws was sorted by the different requirements which were based on a Thompsons Reuters study. Table 1 shows the classification of papers based on their contents. In each category, the number of appropriate articles has been listed in the second column. From the Table 1, it is clear that there were a good number of different research lines.

Fig. 4 showed all elements that effect on security issues in E-health sector. For example, [43] created a hand device which enables a secure and trustworthy path for mobile health devices to effectively communicate with the person wearing it but it was found that there were weaknesses with the device authentication techniques. This suggests a scheme for telemedicine information systems, which will solve the weaknesses of other information systems.

Also, proposes a three-tier architecture for the mobile health applications which uses authentication protocols and data confidentiality so as to preserve the privacy of patients. Green had established necessary procedures for the healthcare finance leaders that must develop good strategies [44]. PHI that were stored, accessed and transmitted via the tablets or phones in the systems monitoring were evaluated and designed through a framework that secures the health monitoring systems despite the common security flaws.

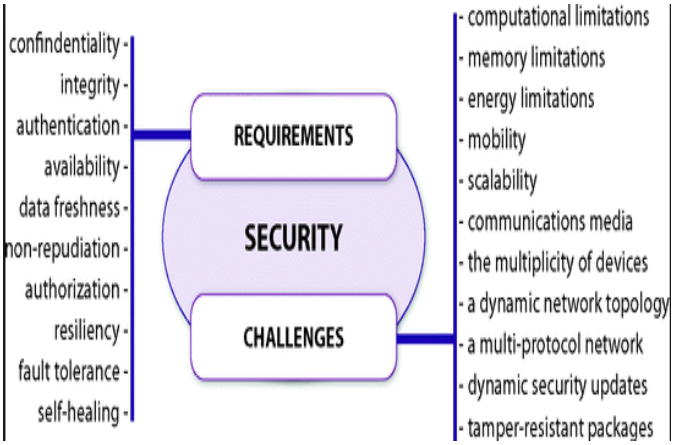

Fig. 4. Internet of Things based E-Health.

TABLE I. CLASSIFICATION OF THE LITERATURE REVIEW RESULTS

Content Type	#Papers
Authentication System/ Technique	19
solution proposal/Secure system	23
privacy and security in cloud computing	23
Privacy and security in the Body Sensor Networks (BSNs)	11
Privacy and security in monitoring systems	14
Privacy and security laws	9
Privacy aspects and General Security	14
Encryption Technique	6
Security in a specific context/place	7
Privacy and security analysis of a system	6
Privacy and security in knowledge evaluation	16
Privacy and security in the mHealth emergency system.	6
Transmission of data security and privacy	5
Privacy and security in the Radio Frequency Identification Systems (RFID)	5
Privacy and security evaluation of systems.	5
Privacy and security in mobile health social networks	6
Security guidelines of mobile health	5
BSNs authentication technique	3
BSNs encryption technique	3
Location privacy	2
Privacy mechanism	2
Health IT review	3
Privacy and security common aspects in applications	3
Data storage secure techniques	2

IV. Discussion

From the results analysis, there are a number of interesting conclusions which can be made. From the results which entail existing laws in the security and privacy of the mobile health, it comes out clear.

That there are no statements which are well defined or there exists no strong lines about the topic both in the United States and the European Union. Most of the laws which are mobile health and information technology related were drafted many years ago. HIPAA was put into law in the year 1996 and applied in the United States while the data protection directive of the European Union was put into law in the year 1995. During those years there were no concepts which could be said to be directly dealing or enforcing on mobile health. The statements from the results have addressed the obsolete technology in a wide range of years and most of the technical staff would only have been applicable in the electronic health field. However, the concepts of electronic health could easily be extended into the mobile health field.

When trying to put the laws in practice of the mobile health field, an issues present is that the laws are too old and too open and as a result need to the reformulated and revised by taking into account the current, industries, technologies and the overall healthcare fields while giving more attention to the mobile applications industry. Despite some of the laws being in enhancement such as the European Union Data Protection Regulation the regulations are by far too general and hence cannot enforce security and privacy of mobile health application to the expectations of many. As a result, it is necessary that rules which are more specific get drafted so that it is made sure that the technical mechanisms for private apps are mentioned so that the common security problems can be solved. By addressing the literature review results, one can easily find out that the fields which were highly researched are those which propose techniques or secure systems that are usually used for privacy and security such as encryption, authentication and data transmission. From the results, there was a special mention of the BSNs techniques and aspects which lately are highly extended [42],[45].

The new ideas are highly important, but there is a considerable field addressing the issue but research has not been done. For example, there are few privacy and security recommendations for the already existing mechanisms and which was one of the paper writing reasons. With mobile health, a lot of research needs to be done on the location privacy, since the violation of healthcare privacy is also a violation of all the general aspects. Articles which addresses privacy and security with mobile health applications deserve a special mention and the reason for this is that health apps are usually created every day but with them there lack privacy and security mechanisms which can effectively maintain the confidentiality of the app users' data. Most of the mobile apps used today lack users' consent collection and privacy policies. From the literature review, there were only seven articles addressing applications that were identified [46].

Three articles were about privacy and security in the general terms while four had proposed guidelines. Albrecht et al. article had very interesting concepts and it was the only article that was proposing for app-synopsis but with some guidelines for designers so that transparent information can be offered about the apps and at the same time presenting vital information on privacy and security information With the considerable amount of information obtained from the literature review, it was highly possible to prepare recommendations for the application designers about privacy and security methods that should be followed towards satisfaction of the United States and European Union satisfaction of laws. However, considering only the minimum requisites could be enough in guiding law observance.

Since PHI must be intensely protected and it is highly sensitive, requisites should be applied. Although certain security mechanism has already been proposed which include RSA, VPN, and AES these are not the only security mechanisms which are to be considered or implemented in the modern technology. There are many more methods which can be even more effective and aim to meet the same standards. The authors selected the three security mechanism identified above because they have been common in a good number of papers and internationally they are well studied. However, it is again important to remember that the final decisions usually depend on the designers or app developers.

For future research, there a good number of research lines. The current work can be extended by studying all those laws which regard security and privacy in other zones such as the Asian countries. For the purpose of coming up with complete recommendations, future researchers should consider looking at more zones and not only the EU and the USA. Much work of this research has been addressed on the privacy and security on m-Health applications, but crucial issues such as interoperability have been left out. As a result, it is good that aspects are combined so as to obtain interoperable secure systems which imply complex studies and processes.

Another future direction in research is the inclusion of recommendations that are proposed in the development of mobile applications so as to evaluate the problems and complexity that appear in processes. However, challenges to be expected are higher workload and processing times for the developers and designers. It is for this reason that they prefer not to integrate these concepts into their apps. Ultimately there is limited awareness is privacy and security law

V. Funding

This research is funded by the Deanship of Research and Graduate Studies in Ajloun National University Ajloun, 26810, Jordan.

References

[1] M. B. Alazzam, Y. M. Al-sharo, and M. K. Al-, "DEVELOPING (UTAUT 2) model of adoption mobile health application in jordan E-GOVERNMENT," vol. 96, no. 12, 2018.

[2] S. Z. Lowry, E. S. Patterson, and M. C. Gibbons, "Technical Evaluation , Testing , and Validation of the Usability of Electronic Health Records : Empirically Based Use Cases for Validating Safety- Enhanced Usability and Guidelines for Standardization NISTIR 7804-1 Technical Evaluation , Testing , and Val."

[3] M. R. Ramli, Z. A. Abas, M. I. Desa, Z. Z. Abidin, and M. B. Alazzam, "Enhanced convergence of Bat Algorithm based on dimensional and inertia weight factor," J. King Saud Univ. - Comput. Inf. Sci., 2018.

[4] H. A. Abdelghaffar and P. Duquenoy, "Studying eGovernment Trust in Developing Nations Case of University and Colleges Admissions and Services in Egypt."

[5] K. Singh et al., "Developing a Framework for Evaluating the Patient Engagement , Quality , and Safety of," 2016.

[6] S. Yang, "Understanding Undergraduate Students' Adoption of Mobile Learning Model: A Perspective of the Extended UTAUT2," J. Converg. Inf. Technol., vol. 8, no. 10, pp. 969–979, May 2013.

[7] M. B. Alazzam, "Physicians' Acceptance of Electronic Health Records Exchange: An Extension of the with UTAUT2 Model Institutional Trust," Adv. Sci. Lett., vol. 21, pp. 3248–3252, Feb. 2015.

[8] H. Rahimi and H. E. L. Bakkali, "A New Trust Reputation System for E-Commerce Applications."

[9] H. Ahmadi, G. Arji, L. Shahmoradi, R. Safdari, M. Nilashi, and M. Alizadeh, The application of internet of things in healthcare: a systematic literature review and classification, vol. 0, no. 0. Springer Berlin Heidelberg, 2018.

[10] H. Li, J. Wu, Y. Gao, and Y. Shi, "Examining Individuals' Adoption of Healthcare Wearable Devices: An Empirical Study from Privacy Calculus Perspective," Int. J. Med. Inform., vol. 88, no. 555, pp. 8–17, 2016.

[11] M. Pekkaya, Ö. P. İmamoğlu, and H. Koca, "Evaluation of healthcare service quality via Servqual scale : An application on a hospital," vol. 9700, no. October, 2017.

[12] R. Shokri, M. Stronati, C. Song, and V. Shmatikov, "Membership Inference Attacks Against Machine Learning Models," Proc. - IEEE Symp. Secur. Priv., pp. 3–18, 2017.

[13] A. Mamra and A. Mamra, "A Proposed Framework to Investigate the User Acceptance of Personal Health Records in A Proposed Framework to Investigate the User Acceptance of Personal Health Records in Malaysia using UTAUT2 and PMT," Int. J. Adv. Comput. Sci. Appl., no. March, 2017.

[14] C. Rivas-echeverría et al., "Features and Applications of an Information System Developed for a Sleep Clinic," pp. 209–215.

[15] A. H. H. M. Mohamed, H. Tawfik, D. Al-Jumeily, and L. Norton, "MoHTAM: A Technology Acceptance Model for Mobile Health Applications," 2011 Dev. E-systems Eng., pp. 13–18, Dec. 2011.

[16] M. Rasmi, M. B. Alazzam, M. K. Alsmadi, A. Ibrahim, R. A. Alkhasawneh, and S. Alsmadi, "Healthcare professionals ' acceptance Electronic Health Records system : Critical literature review (Jordan case study) Healthcare professionals ' acceptance Electronic Health Records system : Critical literature review (Jordan case study)," Int. J. Healthc. Manag., vol. 0, no. 0, pp. 1–13, 2018.

[17] A. Mamra et al., "Theories and factors applied in investigating the user acceptance towards personal health records : Review study Theories and factors applied in investigating the user acceptance towards personal health records : Review study," Int. J. Healthc. Manag., vol. 0, no. 0, pp. 1–8, 2017.

[18] T. Otte-Trojel, T. G. Rundall, A. de Bont, and J. van de Klundert, "Can relational coordination help inter-organizational networks overcome challenges to coordination in patient portals?," Int. J. Healthc. Manag., vol. 10, no. 2, pp. 75–83, 2017.

[19] S. Nikou and H. Bouwman, "The Diffusion of Mobile Social Network Service in China: The Role of Habit and Social Influence," 2013 46th Hawaii Int. Conf. Syst. Sci., pp. 1073–1081, Jan. 2013.

[20] M. B. Alazzam, A. B. D. Samad, H. Basari, and A. Samad, "PILOT STUDY OF EHRS ACCEPTANCE IN JORDAN HOSPITALS BY UTAUT2," vol. 85, no. 3, 2016.

[21] M. B. Alazzam, A. Samad, H. Basari, and A. S. Sibghatullah, "Trust in stored data in EHRs acceptance of medical staff : using UTAUT2," vol. 11, no. 4, pp. 2737–2748, 2016.

[22] S. M.Alazzam, BASARI, "EHRs Acceptance in Jordan Hospitals By UTAUT2 Model: Preliminary Result," J. Theor. Appl. Inf. Technol., vol. 3178, no. 3, pp. 473–482, 2015.

[23] V. Inukollu, S. Arsi, and S. Ravuri, "Security Issues Associated With Big Data in Cloud Computing," Int. J. Netw. Secur. Its Appl., vol. 6, no. 3, pp. 45–56, 2014.

[24] G. Suciu et al., "Big Data, Internet of Things and Cloud Convergence– An Architecture for Secure E-Health Applications," J. Med. Syst., vol. 39, no. 11, 2015.

[25] M. Zineddine and I. Privacy, "automated healthcare information privacy and security : the uae context," vol. 2012, pp. 311–318, 2012.

[26] M. Doheir, B. Hussin, A. Samad, H. Basari, and M. B. Alazzam, "Structural Design of Secure Transmission Module for Protecting Patient Data in Cloud-Based Healthcare Environment," Middle-East J. Sci. Res., vol. 23, no. 12, pp. 2961–2967, 2015.

[27] A. M. Tawfik, S. F. Sabbeh, and T. El-shishtawy, "Privacy-Preserving Secure Multiparty Computation on Electronic Medical Records for Star Exchange Topology," Arab. J. Sci. Eng., 2018.

[28] M. Chen, S. Mao, and Y. Liu, "Big data: A survey," Mob. Networks Appl., vol. 19, no. 2, pp. 171–209, 2014.

[29] S. Trang and S. Zander, "Dimensions of Trust in the Acceptance of Inter- Organizational Information Systems in Networks : Towards a Socio-Technical Perspective," 2014.

[30] M. B. Alazzam, "Big Data Classification: Problems and Challenges in Network Intrusion Prediction with Machine Learning," Int. J. Eng. Technol., vol. 7, no. 4, pp. 3865–3869, 2018.

[31] Y. Mohammad Al-Sharo, G. Shakah, M. Sh Alkhaswneh, B. Zeyad Alju-Naeidi, and M. Bader Alazzam, "Classification of big data: machine learning problems and challenges in network intrusion prediction," Int. J. Eng. Technol., vol. 7, no. 4, pp. 3865–3869, 2018.

[32] X. Xu, "Understanding Users ' Continued Use of Online Games : An Application of UTAUT2 in Social Network Games," no. c, pp. 58–65, 2014.

[33] M. Popescu, G. Chronis, R. Ohol, M. Skubic, and M. Rantz, "An eldercare electronic health record system for predictive health assessment," 2011 IEEE 13th Int. Conf. e-Health Networking, Appl. Serv. Heal. 2011, pp. 193–196, 2011.

[34] A. Reddy, "A study on consumer perceptions on security, privacy & trust on e-commerce portals," vol. 2, no. 3, 2012.

[35] A. S. MB.Alazzam, "Review of Studies With Utaut As Conceptual Framework," Eur. Sci. J., vol. 10, no. 3, pp. 249–258, 2015.

[36] A Zanella, N. Bui, a Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for Smart Cities," IEEE Internet Things J., vol. 1, no. 1, pp. 22–32, 2014.

[37] S. J. Alotaibi and M. Wald, "Evaluation of the UTAUT model for acceptable user experiences in Identity Access Management Systems," 2013 IEEE Third Int. Conf. Inf. Sci. Technol., pp. 232–237, Dec. 2013.

[38] N. M. Kamel Boulos, Maged N; Al-Shorbaji, M. N. Kamel Boulos, N. M. Al-Shorbaji, and N. M. Kamel Boulos, Maged N; Al-Shorbaji, "On the Internet of Things, smart cities and the WHO Healthy Cities," Int. J. Health Geogr., vol. 13, no. 1, pp. 1–7, 2014.

[39] D. J. Kim, Y. I. Song, S. B. Braynov, and H. R. Rao, "A multidimensional trust formation model in B-to-C e-commerce: A conceptual framework and content analyses of academia/practitioner perspectives," Decis. Support Syst., vol. 40, pp. 143–165, 2005.

[40] H. V Jagadish et al., "Big Data and Its Technical Challenges," Assoc. Comput. Mach. Commun. ACM, vol. 57, no. 7, p. 86, 2014.

[41] R. G. Hollands, "Critical interventions into the corporate smart city," Cambridge J. Reg. Econ. Soc., vol. 8, no. 1, pp. 61–77, 2015.

[42] O. Tene and J. Polonetsky, Big data for all: Privacy and user control in the age of analytics, vol. 11, no. 5. 2013.

[43] C. L. Hsu and J. C. C. Lin, "An empirical examination of consumer adoption of Internet of Things services: Network externalities and concern for information privacy perspectives," Comput. Human Behav., vol. 62, pp. 516–527, 2016.

[44] L. M. Telefons, "Mobile Technologies and Services Development Impact on Mobile Internet Usage in Latvia," vol. 1142, 2013.

[45] C. Science, "Toward Privacy-Preserving Emergency Access in EHR Systems with Data Auditing," no. April, 2013.

[46] N. Rahimi and A. Jetter, "Explaining Health Technology Adoption: Past, Present, Future," Manag. Eng. Technol. (PICMET), 2015 Portl. Int. Conf. on. IEEE, pp. 2465–2495, 2015.