2016 9th International Conference on Developments in eSystems Engineering

Mapping Security Requirements of Mobile Health Systems into Software Development Lifecycle

Majid A. Al-Taee, Waleed Al-Nuaimy, Zahra J. Muhsin, Ali Al-Ataby
Department of Electrical Engineering and Electronics
University of Liverpool, Liverpool, UK
e-mail: {altaeem, wax, aliataby}@liv.ac.uk; muhsinzj@gmail.com

Ahmad M. Al-Taee
School of Medicine
Saint Louis University, USA
e-mail: altaeeam@slu.edu

***Abstract*—The shift to delivering mobile healthcare services is inevitable. However, finding effective ways to protect personal health information handled by these systems is still a challenging task even with the utilization of advanced technology and trained professionals. This is mainly due to the fact that the peripheral defense on the Internet and web-based applications does not handle the root causes of the application's vulnerabilities. This paper proposes a solution for enhancing security and personal privacy in electronic/mobile health (e/mHealth) systems through embedding security schemes into software-development lifecycle. The proposed solution, which encompasses various healthcare-specific security needs in mobile health systems, aims at ensuring a balance between personal privacy through ensuring that patients have control over their own information from one side and information sharing that is necessary for integrated service delivery from the other side. This balance is achieved through handling security and privacy challenges through careful design and implementation of data protection mechanisms, cryptography, access control, and auditory that give patients and their health care professionals the right to control disclosures of identifiable health data.**

Keywords—diabetes management; eHealth; mHealth; platform-as-a-service; security requirements; software security

I. INTRODUCTION

Electronic/mobile health (e/mHealth) has an enormous potential to improve quality of care and health service delivery over a distance. In these systems, personal mobile devices enable remote data collection and monitoring for many purposes such as self-management of chronic diseases [1] – [3], medical decision support [4] – [7], elderly tracking [8], online monitoring of patients compliance in diabetes management [9] and other purposes. The growing interest and acceptability of these systems by patients [10] – [11] have also generated new security and privacy concerns [12]. Despite the existence of security technologies, the future will impose additional challenges on security and trustworthiness of these systems due to its pervasiveness and the lifelong involvement of their users.

Most of the existing enterprise security solutions, if not all, are based on utilizing a peripheral defense layer which involves security tools and technologies such as demilitarized zone, firewalls, intrusion detection/ prevention systems [13], denial-of-service prevention [14], tunneling mechanisms [15] and others. Despite the security advantages gained by utilizing these network defense solutions, numerous attacks are still seen every day on the Internet and Web-based applications. This is mainly due to the fact that peripheral defense does not handle the root causes of the application's vulnerabilities. Software vulnerability is defined as [16]; *"A hole or a weakness in the application, which can be a design flaw or an implementation bug that allows an attacker to cause harm to the stakeholders of an application."*

To date, finding effective ways to protect personal health information handled by these systems is still a standing challenge despite the utilization of advanced technologies and trained professionals. If mHealth system fails to safeguard patient privacy, the consequences can be significant; the benefits of the system to patients and health carers could be seriously undermined and reputation of the organization could be jeopardized. The fundamental goals of systems security, which typically involves personnel, procedures and technology, are to detect, recover and prevent violations [17]. This situation can be improved by adopting one (or more) of the existing privacy frameworks [18], [19] and security architectures [20] – [22]. Of these, the security architecture of the ITU-T model X.805 defines dimensions of achieving comprehensive security solutions for distributed applications [23].

Security of cloud applications is essentially a mean of controlling clients' activities in the context of business logic layer, which acts as a mediator between the presentation and backend data layer. This layer is responsible for delivering the requested set of information (data) to a user based on specific business rules/logic. Failure to behave as expected at any stage of the request's lifecycle is considered a control breach that eventually leads to discarding the request, and thus preventing the backend data from any unauthorized access. This objective can only be met when security requirements are dealt with as an integrated part of the software development lifecycle (SDLC) [24] – [26]. Furthermore, in cloud applications development, the close collaboration between application developers and security specialists during the SDLC is therefore critical to remove software vulnerabilities that lead to information security failures.

In this paper, the e/mHealth-specific security requirements are identified and implemented throughout different phases of the development lifecycle of mHealth system for diabetes mellitus self-management support. The proposed solution aims to ensure a balance between personal privacy and information sharing that is necessary for integrated service delivery.

The remainder of this paper is organised as follows: Section II provides network overview architecture for the mHealth system under study. Section III describes the

978-1-5090-5487-9/17 $31.00 © 2017 IEEE
DOI 10.1109/DeSE.2016.16

proposed layered security approach. The core implementation of various security dimensions through the SDLC is presented in Section IV. The obtained results are presented and discussed in Section V. Finally; the work is concluded in Section VI.

II. System Overview

The mHealth system under study, which was previously reported in [1], can be best described as a policy-based object category within the context of emerging Internet-of-Things paradigm. Its design is driven by the needs of integrated diabetes care [27] which embeds behavioral, social and economic dimensions within the current routine care of diabetes with the ultimate goal of improving health outcome of the self-management process. The system allows diabetics to and their health care professionals to monitor the self-management blood glucose (BG) measurements. It has been acknowledged that patients' access to their self-care data helps making informed decisions on BG control and improves quality of life. However, patients need to be confident that personal health information systems are secure as well as well protected from unauthorized access and misuse by others. Fig. 1 shows abstract network architecture for the mHealth system under study. It consists of a physical-objects (POs) layer (i.e. medical devices, smartphones as well as patients and their health carers) and a cloud layer, which in turn consists of two main sub-layers; a disease management hub (DMH) and central data storage (DS). The PO and cloud layers are linked by an existing telecom network infrastructure, as illustrated. The main components of these layers are outlined as follows.

A. Physical-Objects Layer

This layer represents the patient's hub; it comprises physical data collection nodes (N_1, N_2 … N_n) where n represents the total number of registered patients. Each node comprises a mobile device linked to a set of medical sensors, including: blood sugar monitor, blood pressure monitor, and a weight scale, as illustrated in Fig. 1. The mobile device communicates with the medical sensors to collect the patient's measurement using Bluetooth connectivity. The collected measurements and other patient's data relevant to diabetes care (e.g. diet, exercise, illness conditions, etc.) are then encrypted and uploaded to the patient's medical record at a remote DMH server for further processing and monitoring purposes.

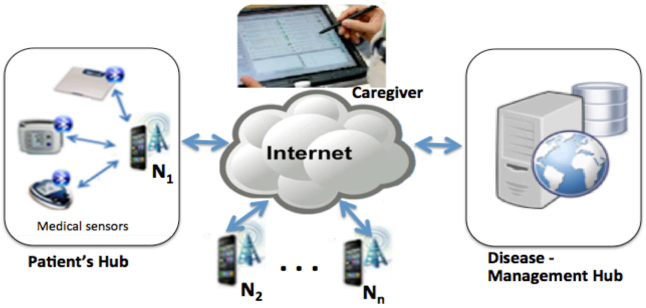

Figure 1. Abstract network architecture of the mHealth system [1]

B. Cloud Layer

This layer represents central disease management hub and central data storage. It encompasses logic of disease management support and back-end data storage. This hub is accessible by human objects (i.e. patients and their caregivers) and device objects (i.e. mobile devices). Each of these objects can access system services based on authentication credentials and pre-defined authorization privileges, depending on their roles.

III. Layered Security Approach

Unlike other healthcare systems, mHealth allows for continuous collection of personal information. In the context of integrated diabetes care [27], it does not only collect medical information but also gathers data about psychological, lifestyle, location, and social interactions. Furthermore, it enables a broader range of personal data sharing with professional caregivers, insurance companies, family members, and others. However, this makes personal privacy protection more complex when compared to other healthcare information systems.

Security requirements of the system under study are based on the Platform-as-a-Service (PaaS) cloud in which the service model encompasses the security of the cloud service provider (CSP) as well as the system software and hardware layers. These layers describe the communication channels, the platform on which the applications are developed, and the hardware resources that support the software layers [29]. Security issues related to the system therefore vary from technology-based to security responsibilities shared between the CSP and system users.

A. Security Objectives and Requirements

Three security objectives are defined by the Federal Information Security Management Act (FISMA) for information systems [29]; confidentiality, integrity, and avaiability. Potential levels of impact for each of these security objectives were also categorized into into low, moderate or high. Definitions of these impact levels are given in Table I. These potential impacts to security objectives in PaaS model are used to specify security requirements of the mHealth system under study. In order to facilitate elicitation of the security requirements, the system is segregated into three separate layers; physical objects layer, disease management logic and back-end data storage, as illustrated in Fig. 1. The latter two layers are sub-layers of the original cloud layer, as described earlier. This segregation enables the identification of the security mechanisms required for securing components that provide computing, network and storage services. The CSP and/or the physical-layer objects can access or manage each of these layers depending on the development attributes (i.e. Private, Public or Hybrid) of their software modules.

The security requirements at each layer are classified into four levels (vital, intermediate, basic and none). These levels are then assigned numeric values of 3, 2, 1 and 0, respectively. The system stakeholders can therefore use these numbers to classify their security requiremnts to meet their security objectives in terms of the impact levels. These requirements are initially collected from the system stakeholders and then used to generate quantitative data necessary for identifying critical areas in the system layers where security mechanisms should be implemented to meet individual security requirements. The system stakeholders, software developers and CSP can therefore align the anticipated security requirements with the security classification levels to reduce potential risks. The proposed security classification levels and their objectives, requirements, and potential impacts (if compromised) on the system's stakeholders are summarised in Table I.

TABLE I SECURITY CLASSES, OBJECTIVES AND IMPACT

Security Class	Objective	Description	Impact
Vital	Protecting the confidentiality, integrity and availability of sensitive data.	• Multilevel security mechanism that allows the cloud architecture to protect itself from unauthorized access and recovers quickly when under attack. • A security mechanism with multi-factor authentication including a biometric method of authentication. • The security mechanism must also consist of more than one access control policy.	Severe
Intermediate	Preserving the confidentiality, integrity and availability of data in transit and at rest on the cloud environment.	• A security mechanism that consists of multi-factor authentication methods including a non-biometric identification method. • The mechanism must also consist of at least one access control policy.	Moderate
Basic	Preserving the confidentiality, integrity and availability of data in transit and at rest on the cloud environment.	A basic security describes the implementation of: • Proprietary encryption with at least 128-bit shared. • Authentication and key exchange with at least 1024-bits encryption algorithm. • Certificate issued by third party. • Master or key encryption keys managed locally with access control policies.	Acceptable
None	Preserving the confidentiality, integrity and availability of data is either not required or not applicable.	No security mechanism is required.	None

B. *Security Domains*

Operational security on PaaS cloud models implements four security domains [30], [31]: (i) Identity and Access Management (IAM), (ii) Encryption and Key Management (EKM), (iii) Virtualization Security Management (VSM), and (iv) Database Security Management (DSM) in addition to the Network Security Management (NSM) as a fifth domain. The latter domain covers security of the communication channels within and between different system layers. These domains that represent the security requirements of the system stakeholders are considered adequate to govern the security needs for the system under study. The system layer of critical security requirements (CSR) can be identified by mapping the chosen security classes for each of these security domains into a security matrix, as shown in Table II. This matrix consists of the following aspects:

- System architecture layers; physical objects (POs), disease management (DM) hub and the central data storage (DS).
- The entity responsible for managing or implementing security controls on each layer of the cloud depending on the cloud deployment model (managed, semi-managed or unmanaged).
- Security requirements; values (0 - 3) that correspond to the security classifications given in Table II are provided by the system stakeholders for each requirement classification (R_1 – R_5) in the columns and rows provided.
- Critical security requirement; this section comprises of the sum of the security requirements (R_1 – R_5) on each row, as illustrated.

The identified security requirements can be met by: (i) appropriate choice of the deployment model (i.e. private, hybrid, and public) and (ii) embedding these requirements, as applicable, throughout the SDLC of various applications/services at both the POs and cloud layers. The latter implementation, which is of a particular interest in this work, is described next in Section IV.

TABLE I1 SECURITY REQUIREMENTS MATRIX

System Layer	Security Requirements					CSR
	IAM	EKM	VSM	DSM	NSM	
Physical objects	R_1	R_2	R_3	R_4	R_5	$\sum_{i=0}^{5} R_i$
Disease-management logic	R_1	R_2	R_3	R_4	R_5	$\sum_{i=0}^{5} R_i$
Data storage	R_1	R_2	R_3	R_4	R_5	$\sum_{i=0}^{5} R_i$

IV. SDLC-BASED SECURITY IMPLEMENTATION

The core implementation of the proposed security solution focuses on embedding the identified security requirements into SDLC of both the POs and cloud layers. The various applications hosted by these layers are secured through classifying attributes of the underpinning software implementation of these applications into secure (i.e. private or protected) and non-secure (i.e. public). Fig. 2 shows abstract security architecture for the mHealth system under study. Implementation of the security requirements, specified earlier in Section III, can be described as follows.

A. *Encryption and Key Management*

System users are classified into two categories; browser-based clients (i.e. human users) and non-browser clients (i.e. smartphones). As illustrated in Fig. 2, the former category of clients use secured Hypertext Transfer Protocol (HTTPS) to secure their communications with the cloud layer. HTTPS adds the security features of SSL/TLS protocol to the unsecure HTTP protocol. However, the HTTPS is not supported by the non-browser clients.

Long-range connectivity between mobile devices and the cloud server is based on periodic database synchronization events through which patients measurements and other information are uploaded to the central database at the cloud. Simultaneously, any feedback (e.g. health info, advices, warning, motivation messages, etc.) that is either assigned by the caregivers or automatically generated by the system is downloaded to the patient's mobile device. In this healthcare scenario, the mobile device acts as a master device to initiate this periodic data synchronization. No HTTP requests are expected from the cloud end and thus, all applications deployed on the physical layer smartphones are protected from the risk of external access during their communication with the cloud. Despite this security advantage, the synchronization is potentially vulnerable to the "man-in-the-middle" security threat recalling that device clients do not support the native HTTPS.

To secure periodic database synchronization, a new symmetric-key cryptography algorithm is proposed and implemented at the communication modules developed at both the smartphone and the cloud server. Unlike equivalent algorithms [32], [33], the proposed cryptography does not include full authentication data in the transmitted packets between the two ends. Instead, it distributes the encryption/decryption key between three entities; the user, mobile device, and the cloud server. In addition, the token used to encrypt/decrypt data at both ends is neither transferred with the packets nor the authentication data, thus maintaining robust communication channel security. Management of the encryption/decryption key can be explained with reference to the message sequence diagram of Fig. 3, as follows.

1) Key generation: At first use, the mobile device generates a 4-digit PIN code. The user (patient) will then register this PIN code as well as the mobile device serial number into his/her account at the remote DMH.

2) Key activation: At second use, the mobile device attempts to establish a connection with the DMH using the generated PIN. If successful, the cloud server returns an encrypted key (called access key), which allows the mobile device to access certain services on the DMH.

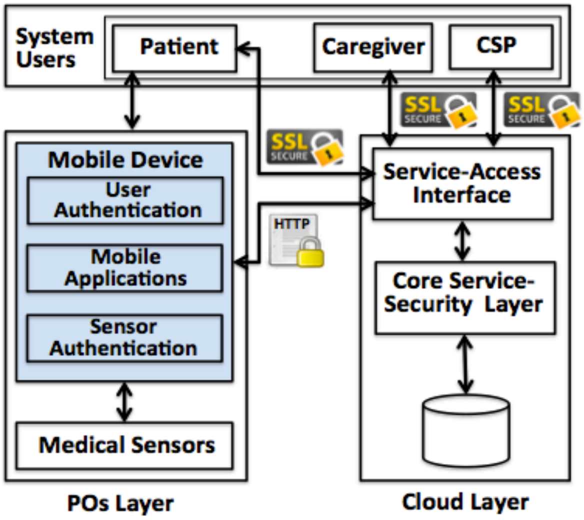

Figure 2. Abstract security architecture of the mHealth system

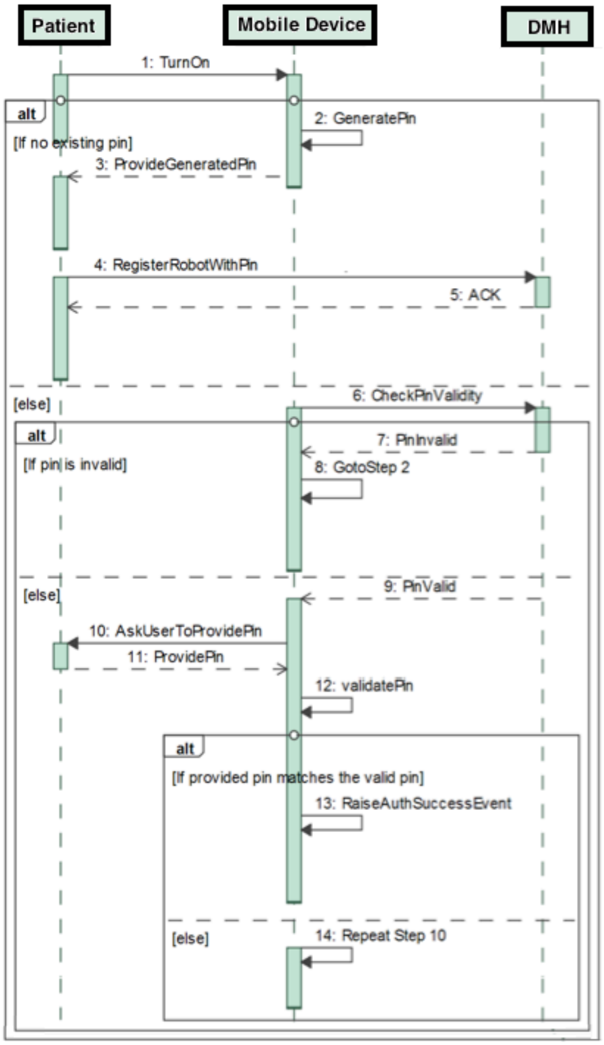

Figure 3. Authentication process for mobile devices

3) Access key: The access key is used to encrypt/decrypt all data exchanged between the mobile device and the cloud server during the periodic data synchronization process. The user can deactivate the access key through the user account at the cloud layer. The system also deactivates the key after several unsuccessful consecutive attempts. Once deactivated, steps 1 and 2 should be repeated to authenticate the device again.

B. Identity and Access Management

Fig. 4 shows a security architecture for various software modules in which various security requirements are implemented. The security related modules that are embedded throughout the SDLC of the disease management and data storage applications at the cloud layer are described briefly in Table III. For example, authentication of users and devices as well as data integrity requirements are implemented in the service access interface; service validation in the service-request handler; user authorization and database access control in the privileged-access manager; non-repudiation in the public and secure services as well as in the database server interface where all transactions are logged. Implementation of security dimensions in the cloud layer spreads over several software classes including a service class, data validation class, application service class and application security class. Each of these classes has specified security functions; for example, the latter class implements security functionalities that identify who are logged in, which profile(s) is being viewed, and whether or not the logged in user(s) is allowed to access a certain service(s).

The system audit will then automatically notifies the patient through his/her mobile device of any access or amendments made in his health profile. This will not only timely notify patients of any changes in their treatment plan but also protects their confidentiality and offers them the right to control disclosures of their identifiable health data through their accounts at the cloud layer by specifying a set of desired security attributes.

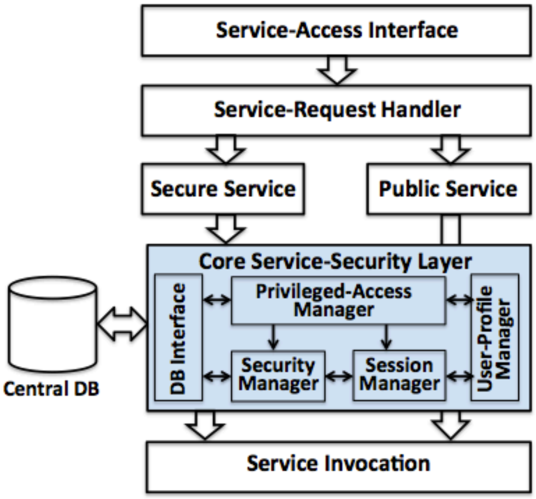

Figure 4. Security architecture of the cloud layer

TABLE III SECURITY-RELATED MODULES OF THE CLOUD LAYER

Component	Description
Service Access Interface	All requests are handled through a unified access interface that loads all other modules and passes the request to the service-request handler module.
Service Request Handler	Verifies request completion and dispatches the request into either a public or secure execution stack.
Public Service	The service will only be looked up in the public services dictionaries and if a service is found to exist it will be sent to the invocation process. If a certain requested service doesn't exist, the server discards the request.
Secure Service	Before having the service looked up in the private services dictionary, the request is sent to the privileged-access manager which in turn will communicate with both the session- and security-managers to validate identity and authorization privileges of the requester prior to grant access to the required service.
Privileged-Access Manager	It uses both the security and session managers to authenticate the request and validates user login. This involves database check to match a session-encrypted key against the database.
Security Manager	Data validation, decryption, and hashing
Session Manager	Manages session, cookies data, and tracks user logins
User-Profile Manager	It controls access to system services based on the profile categories of the users (i.e. patient, caregiver, CSP admin, etc.). For each category, the system specifies set of privileges that are granted or revoked by a higher-privileged user profile. For example, the highest-privilege profile is given to the super CSP admin amongst the technical-support team and the physician is given the highest-privilege profile amongst the caregivers team. In this hierarchical access-privilege structure, the patient is given the least privileged profile. System services cannot be invoked unless the attributes of requester profile match the requested service.
DB interface	Upon successful validation of the requester and service attributes, this interface grant access to the central database schema to retrieve or store data.
Service Invocation	The actual execution of the service takes place and the results are sent back to the browser.

V. RESULTS AND DISCUSSION

Data collected from 22 users relevant to the classification of security requirements showed that the data-storage layer with a summation of 11 points (50%) represented the most critical area in the cloud layer. The disease management logic scored 7 points (31.8%) while the physical-objects layer is found to be with a summation of only 4 points (18.2%), as shown in Fig. 5.

Privacy and security of the patient's data can therefore be considered a crucial dimension to the success and full flourish of the e/mHealth systems. From the users perspective, security of the cloud-based resources was found to be of a particular importance (81.8%) as compared to the data resources at the physical layer (18.2%).

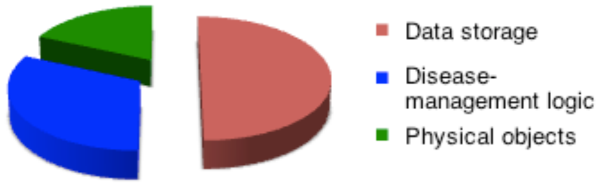

Figure 5. Prioritization of security requirements

VI. Conclusions

We have studied the capabilities of different adversaries and proposed implementing e/mHealth-specific security requirements throughout the different phases of the software development lifecycle. This approach is expected to complement existing peripheral defense security layer with the ultimate goal of maintaining a balance between personal privacy and information sharing that is necessary for integrated service delivery. The close collaboration between the application developers and security specialists during the SDLC is therefore critical to remove software vulnerabilities that can lead to information security failures. However, implementation of this approach is still open for further studies. For example, a wider study is required to assess its impact on the system security when implemented with and without utilizing network-defense solutions. The organization perspective is another important dimension that needs to be studied since the proposed approach may require additional security-knowledgeable resources.

References

[1] M. A. Al-Taee, W. Al-Nuaimy, Z. J. Muhsin, A. Al-Ataby, ”Robot assistant in management of diabetes in children based on the Internet of things,” IEEE Internet of Things Journal, vol. 4, 2016. doi: 10.1109/JIOT.2016.2623767.

[2] M. A. Al-Taee, W. Al-Nuaimy, Z. J. Muhsin, A. Al-Ataby and S. N. Abood, “Mobile health platform for diabetes management based on the Internet-of-things,” IEEE Jordan Conf. on Applied Electrical Engineering and Computing Technologies, Amman, Jordan, 3-5 November 2015, pp. 1-5.

[3] M. A. Al-Taee, and S. N. Abood, “Mobile acquisition and monitoring system for improved diabetes management using emergent wireless and web technologies,” Int. Journal of Information Technology and Web Engineering, vol. 7 (1), 2012, pp. 18 – 32.

[4] M. A. Al-Taee, A. Zayed, S. N. Abood, M. A. Al-Ani, A. M. Al-Taee, and H. A. Hassani, “Mobile-based interpreter of arterial blood gases using knowledge-based expert system,” Int. Journal of Pervasive Computing and Communications, vol. 9 (3), pp. 270-288.

[5] A. Y. Al-Hyari, A. M. Al-Taee and M. A. Al-Taee, “Diagnosis and classification of chronic renal failure utilizing intelligent data mining classifiers,” Int. J. of Information Technology and Web Engineering, vol. 9 (4). 2014, pp. 1-13.

[6] A. M. Al-Taee, M. A. Al-Taee, W. Al-Nuaimy, Z. J. Muhsin, and H. AlZubi., “Smart bolus estimation taking into account the amount of insulin on board,” IEEE Int. Conf. on Computer and Information Technology, Liverpool, UK, 26-28 October 2015, pp. 1051-1056.

[7] M. A. Al-Taee, S. N. Abood, W. K. Al-Nuaimy and A. M. Al-Taee, “Blood-glucose pattern mining algorithm for decision support in diabetes management,” Proc. 14th UK Workshop on Computational Intelligence, Bradford, UK, 8 – 10 September 2014, pp. 1-7.

[8] X. Xiao, A. K. Wong, K. T.Woo, and R. S-K. Cheng, “An energy-efficient elderly tracking algorithm,” Proc. 2011 IEEE Int. Conf. on Communications (ICC’2011), 5-9 June 2011.

[9] A. M. Al-Taee, A. Al-Taee, Z. J. Muhsin, M. A. Al-Taee, Waleed Al-Nuaimy, “Towards developing online compliance index for self-monitoring of blood glucose in diabetes management,” Proc. 9th Int. Conf. on Developments in eSystems Engineering (DeSE ’2016), Liverpool & Leeds, England, 31st August – 2nd September 2016.

[10] M. A. Al-Taee, R. Kapoor, C. Garrett, and P. Choudhary, “Acceptability of robot assistant in self-management of type 1 diabetes in children,” J. Diabetes Technology and Therapeutics, vol. 18(9) 2016. doi: 10.1089/dia.2015.0428.

[11] M. A. Al-Taee, S. N. Abood, P. Choudhary, C. Garrett and R. Kapoor, “Feasibility and acceptability of robot assistant in self-management of type 1 diabetes in children,” 53rd Annual Conference of the European Society for Pediatric Endocrinology (ESPE2014), Dublin, Ireland, 18-20 September 2014.

[12] M. Meingast, T. Roosta, and S. Sastry, “Privacy issues with health care information technology,” Proc. 28th IEEE EMBS Annual Int. Conf., August 2006.

[13] K. Scarfone, and P. M. Mell, "Guide to intrusion detection and prevention systems (IDPS)," U.S. National Institute of Standards and Technology, Special Publication (NIST SP) - 800-94, 2007.

[14] B. B. Gupta, R. C. Joshi, and M. Misra, “Distributed denial of service prevention,” International Journal of Computer and Electrical Engineering (IJCEE), vol. 2 (2), 2010, pp. 268-276.

[15] A. J. Ghazali, W. Al-Nuaimy, A. Al-Ataby, M. A. Al-Taee, “Building IPv6 based tunneling mechanisms for VoIP security,” IEEE International Multi-Conference on Systems, Signals and Devices, Leipzig, Germany, 21-24 March 2016, pp. 171 – 176.

[16] The Open Web Application Security Project (OWASP), available at: https://www.owasp.org/ index.php/ Main_Page (Accessed on 25 May 2016).

[17] G. Horacio, R. Caceres, and Y. Teshigawara, “Security guideline tool for home users based on international standards,” Information Management and Computer Security, vol. 18 (2), pp. 101-123, 2010.

[18] D. Kotz, S. Avancha, and A. Baxi, “A privacy framework for mobile health and home-care systems,” Proc. 1st ACM workshop on Security and Privacy in Medical and Home-Care Systems (SPIMACS’09), 2009, pp. 1-12..

[19] M AlZghoul, M. A. Al-Taee , and A. M. Al-Taee, “Towards nationwide electronic health record system in Jordan,” IEEE International Multi-Conference on Systems, Signals and Devices, Leipzig, Germany, 21-24 March 2016, pp. 650 – 655.

[20] International Telecommunication Union, “Security in telecom and information technology,” available at http://www.itu.int/itudoc/itu-t (Accessed 20 July 2016).

[21] International Telecommunication Union, Telecommunication Standardization Sector, “Security architecture for systems providing end-to-end communications,” ITU-T Rec. X.805, Oct. 2003.

[22] Cloud Security Alliance, “Security guidance for critical areas of focus in cloud computing V3.0,” Cloud Security Alliance, vol. 3, pp. 155, 2011.

[23] I. Almomani and H. Zedan, “End-to-end security solution for wireless mobile ad hoc network,” Proc. IADIS Int. Conf. Applied Computing, Salamanca, Spain, 18 – 20 February 2007.

[24] A. K. Gupta, U. Chandrashekhar, S. V. Sabnis and F. A. Bastry, “Building Secure Products and Solutions,” Bell Labs Technical Journal 12(3), pp. 55–64, 2007.

[25] M. Paul, “The ten best practices for secure software development”, Information System Security Certification Consortium, Inc, USA, available at https://www.isc2.org/ uploadedFiles/ (ISC)2_Public_Content/Certification_ Programs/CSSLP/ISC2_WPIV.pdf (Accessed on 24 June 2016).

[26] M. I. Daud, “Secure software development model - a guide for secure software life cycle,” Proc. Int. MultiConference of Engineering and Computer Scientists, vol. I, Hong Kong, March 17 – 19, 2010.

[27] M. A. Al-Taee, A.H. Sungoor, S.N. Abood, and N.Y. Philip, “Web-of-things inspired e-Health platform for integrated diabetes care management”, IEEE Jordan Conf. on Applied Electrical Engineering and Computing Technologies, Amman, Jordan, 3-5 December 2013., pp. 1-6.

[28] T. Mather, S. Kumaraswamy, and S. Latif, “Cloud security and privacy, vol. 1, 2009.

[29] S. Zevin, “Standards for security categorization of federal information and information systems,” DIANE Publishing, 2009.

[30] Daniele Catteddu and Giles Hogben, “European Union Agency forNetwork and Information Security: Cloud Computing Risk Assessment,” 2009.

[31] A. Akinbi and E. Pereira, “Mapping security requirements to identify critical security areas of focus in PaaS cloud models,” Proc. IEEE Int. Conf. on Computer and Information Technology, Liverpool-UK, 26-28 October 2015.

[32] N. Qasraw, M. Al-Taee, M. I’emair, M, and R. Al-Asa’d, “Multilevel encryption of plaintext messages using a smart card connected to PC parallel port,” Proc. 3rd Int. Conf. on Modeling, Simulation and Applied Optimization, Sharjah-UAE, 20 - 22 January 2009, pp. 1-6.

[33] M. A. Al-Taee, N. H. Al-Hassani, B. S. Bamajbour, and D. Al-Jumeily, “Biometric-based security system for plaintext e-mail messages,” Proc. Int. Conf. on Developments in eSystems Engineering, Abu Dhabi, UAE, Dec. 14 – 16, 2009, pp. 202 – 206.