Indian Journal of Science and Technology, *Vol 9(S1), DOI: 10.17485/ijst/2016/v9iS1/106842, December 2016*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Passwordless Authentication in Mobile e-health using a Secure Boot Non-regenerated Unique Identity and NFC

Nazhatul Hafizah Kamarudin*, Yusnani Mohd Yussoff and Habibah Hashim

Electrical Engineering Department, University Technology MARA, 40450 Shah Alam, Malaysia;
azzfie@gmail.com, yusna233@salam.uitm.edu.my

Abstract

Mobile e-health is a current application where people can connect with healthcare services through sensor nodes and wireless communication. Existing e-health architecture depends on a third party server in order to get connected with the hospitals. Therefore, it adds up to a security hole in the e-health architecture. Objectives: The objective of this paper is to develop a secured password less authentication protocol for mobile e-health system and to eliminate the need for a third party server. Methods/Statistical Analysis: A non-regenerated unique identity for the e-health sensor node is generated through a secure boot process and the unique value will be used as the sensor node identity. EHEART prototype is designed and e-health server is established. Near Field Communication (NFC) ring is used in this mobile e-health system to enhance the security layer of the proposed authentication protocol. Study was conducted in a closed environment with no exposure to attackers. Findings: The project results demonstrate the development of a secured passwordless authentication for e-health system. By implementing the near field communication in the e-health system, it can reduce the energy consumption where the Bluetooth module will only be automatically turned on when the mobile device is being touched by the NFC ring. EHEART application does not need any username and password combination for login request and authentication process. Formal analysis method AVISPA and SPAN is used to analyse the reliability and the security of the proposed system and it is proven to be secured from replay attack, node cloning and password break attack. Application/Improvements: The outcome form the research will ensure secure connectivity or environment in the e-health monitoring system without depending anymore on a password and third party server. NFC ring in the system will help reduce the power consumption of the mobile device.

Keywords: Mobile e-health, Passwordless Authentication, Secure Boot, Unique Identity

1. Introduction

E-health monitoring system is a healthcare application supported by electronic process and wireless sensor network communication[1]. Mobile e-health is currently a develop technology where people nowadays can connect to the healthcare centre through medical body area network sensors and mobile devices. However, a strong and secure authentication needs to be implemented in the network system since highly sensitive and private data is transmitted through the mobile device. Due to the high demand in e-health, its authentication has become the main concern in the network system since it will display and transmit patient data to the healthcare server. E-health communication system is currently being developed due to the enhancement of the Internet of Things (IOT). Protecting the wireless sensor network of e-health system should be taken as a serious issue in handling the e-health security aspects such as sensor node authenticity and data confidentiality. Current e-health systems mostly implement a default security mechanism which uses username and password combination for authoriza-

*Author for correspondence

tion. However, user tends to have difficulty to remember the username and password combination especially the senior citizens. Besides, the system is vulnerable to password break and man-in-the-middle attack. Username and password has been proven insecure since the password can be cracked by the adversary[2].

The main issue in the e-health system is the authentication scheme and therefore we need to eliminate the need for username and password combination in the current authentication process. Hence, the main purpose of this research is to design an inviolable passwordless authentication security protocol that will be implemented in mobile e-health system which consists of wireless medical sensor nodes that transmit highly sensitive data and extremely susceptible to security attacks. Detailed studies have been conducted to design a soundly and inviolable authentication protocol based on the unique identity of a sensor node generated through a secure boot process and to implement Near-Field Communication (NFC) system in mobile e-health. One of the significant outputs in this research is a secure process of generating a unique identity of a sensor node that will be used as the identity in the e-health authentication protocol in order to improve the security and confidentiality of the e-health system. This research aims to produce a unique identity that will be impossible to be cloned or to be regenerated in order to protect the whole mobile e-health system from security attack mainly node impersonation attack and replay attack. For that reason, this paper proposes a passwordless authentication in mobile e-health system using a unique identity-based authentication and NFC system. The significance of this proposed protocol is to implement a seamless authentication for e-health related applications. This paper designs a new authentication protocol in order to enhance the security of the e-health system.

Username and password combination scheme is the most frequently used for mobile e-health authentication and it is susceptible to identity and password hacking. These recent years, many cases on health data leakage and security attacks have been reported to the Office of Inspector General (OIG) Healthcare Inspection[3]. By using this username and password scheme for identity verification in mobile e-health, a user has to successfully log in into the system and it is an essential part of current e-health authentication schemes in order to protect the e-health applications from security attacks[4,5]. The use of username and password has been proven to be vulnerable to password break attack, unauthorized data access, and man-in-the-middle attack[6,7]. Additional security mechanism should be implemented to increase the security protection in e-health system since username and password can be cracked or shared through debuggers and therefore it is no longer reliable[8]. Authentication is a door to the whole e-health system and it is very important in validating the user identity in order to get an access to the network[9]. The development in internet communication particularly Internet of Things (IOT) has increased the possibility of new security potential treats and the vulnerabilities to the e-health system. Therefore, it is very important to protect the security of the personal data in e-health server[9–11]. In a security mechanism, a service may contain many security schemes and they might have many cryptographic algorithms in order to encrypt and decrypt the data[12]. E-health security requirement is basically on the ability to authenticate and to verify the sensor, the data, access control and the integrity of the data. It is to make sure that there is no manipulation in the data storage and during the communication. Therefore, the health data is only for the authorized user and should be kept safely[13]. Authentication using username and password is a basic and common access authentication for user to make an access request into the network.

Other than username and password combination scheme, role of a third party server in mobile e-health current architecture will also reduce the reliability and the security of the whole system. It is very crucial to maintain high privacy and to protect confidentiality in the e-health data system and we should not reveal health data of the user to any third party server[14]. A major drawback of the shared architecture in e-health system is different users will have the same role and provide the same services to the targeted patient. Therefore, a new method should be created in order to eliminate the problem of having a shared architecture in e-health network system[15]. In the current e-health architecture, mobile device needs to transfer the data through a third party server first before it can get connected to the hospital server[16]. Consequently, people do not trust the level of security implemented in the system and the reliability of sending the e-health data since high privacy and confidential data are being transmitted[17]. Developing security protocols in mobile e-health system is highly needed in order to improve the security system. The e-health network system consists of medical sensor nodes, mobile device, data server and medical centre. Basically, the e-health architecture provides a third-party service provider for data usage[18]. Based

on a review from the Institute of Medicine (IOM), health systems nowadays are having issues to reduce operational cost which are frequently caused by systematic errors and therefore it shows the high need of improving the quality of the e-health system[19]. In transferring the data and sharing the information, there will be several attacks involved in the system. The user especially the patients can expose their user identity and personal information and also exposed the medical information[19,20]. It is important to organize the communications between the user and e-health service provider in order to enhance the quality and the security of the e-health system[21]. Wireless sensor network and wearable sensor in body area network can be integrated in ubiquitous computing to enhance the development of e-health system[22].

In order to accomplish the high security in e-health monitoring system, we should integrate several security mechanisms in the system for instance incorporating two security schemes in the e-health network system[20]. In order to deal with the security issues in e-health network, we should know what are the assets that we want to keep and what are the vulnerabilities of the system as well as the possible threats that can happen in the hardware, software and data system[23].There are a lot of mobile health system that has been already in practical applications, by combining and integrating a wearable or implanted devices and embedded processor to accomplish certain application in healthcare[24].The emerging of the information and communication technology (ICT) and healthcare technology, nowadays personal medical records can be kept and shown through mobile devices[25]. Mobile e-health consists of a set of body sensor connected to a mobile device and then will communicate to an e-health server. The doctors can access the medical data at any time from the mobile device[26]. Security features of the e-health network system is quite critical and based on the research studies in several countries like United States, Denmark, New Zealand, and Germany, people stated their concern on their e-health data security and it is estimated that 25 million required authorization in the disclosure of e-health records system[27]. There have been several security attempts in the e-health system for instance the involvement of the computer access and the duplication data to various e-health hospitals and therefore threatens the e-health medical system[28]. People have been aware of the potential threats in the shared data in e-health system. For example, in Austria, each person can decide whether they want to share their personal information in e-health network with the medical center or not[3].The lack integration between the ICT application and work practical in e-health network system is one of the reasons for ineffective execution and implementation of the mobile e-health system[29].

2. Methodology

A secure password less authentication using a non- regenerated unique identity and near field communication is proposed to eliminate the need for e-health service provider and thus enhance the security of the network system. The main objective of this research is to design and to develop a seamless authentication for e-health monitoring system. By using ATMEGA328P with Bluetooth module and pulse Sensor SEN_11574, a secure password less authentication for mobile e-health monitoring application that can receive data from medical devices is activated and near field communication is utilized. The medical device will transfer heart rate data to android application using Bluetooth in the range of 5 to 10 meters. The pulse sensor can only be clipped on a fingertip. This section discusses through the development of authentication less for e-health monitoring system and it is divided into two major sections which are hardware and software development. The communication between the embedded system and mobile device are based on Bluetooth communication. EHEART application is designed for mobile e-health monitoring system consists of a pulse sensor, a battery source, and Bluetooth module HC-05 that will be the output mechanism for the e-health system to transfer the data to the mobile device. Then, the data from the mobile phone will be sent to the e-health server for further analysis. The system microcontroller is Atmega328P will read input data from pulse sensor and send it to the mobile application via Bluetooth module. Atmega328p microcontroller will be the brain of the whole system. It requires an external 16MHz and 5V power supply to get this microcontroller to be working properly[30].

For identity verification, the NFC ring must be at the back of the mobile phone in order to be verified throughout the authentication process. On mobile device application, it will show the pulse rate of the user or a patient and the setting of the device connection. The assembly language for program coding is used on a Windows OS. The program coding will be transferred to the e-health system microcontroller which is ATMEGA328P. Near field

communication is a form of no physical contact communication between devices. Figure 1 show the architecture of Atmega328p and the PCB layout of the system hardware. The schematic and PCB layout design is the first step of development hardware process of the EHEART system.

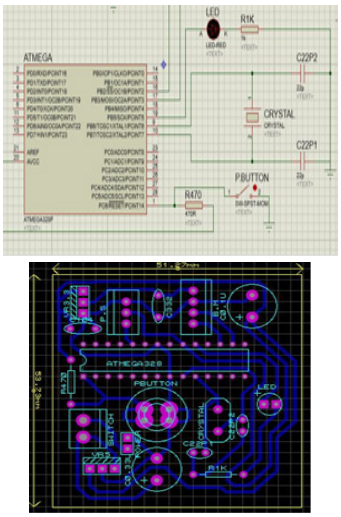

Figure 1. Hardware layout of Atmega328p for EHEART application.

Bluetooth communication is used for the data transmission module between EHEART application and a mobile phone. The mobile platform is able to support Bluetooth module and thus enables the device to receive data from embedded medical sensor device. Bluetooth module receiver will be connected to the Atmega328p transmitter and Bluetooth module transmitter will be connected to the Atmega328p receiver. This EHEART medical device will be attached to the user and pulse sensor SEN_11574 is used to monitor the user data reading by simply clip the pulse sensor to the user fingertip. It can be connected to the mobile phone through Bluetooth using EHEART application and the authorization is made by the user using NFC ring communication. This communication allows a user or a patient to send their identity information without going through multiple steps of setting up a connection. NFC ring can be used together in the authentication process in addition to the sensor node unique identity verification. Therefore, EHEART application uses multi factor authentication and NFC ring implementation can also reduce the power consumption of the mobile phone since it will only turn the Bluetooth module on upon authentication process. It is an electronic ring to turn the Bluetooth on and open the EHEART application on the mobile phone. NFC ring type A (ISO.IEC 14443) is used in this EHEART application. Figure 2 depicts the communication from the NFC ring to a mobile phone application in e-health authentication process.

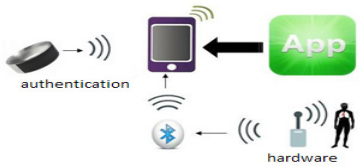

Figure 2. Near field communication ring authentication.

Since the conventional method which is the username and password combination has been proved to cause lots of security problems and user problems especially for elderly users, the usage of NFC ring can really improve the e-health communication system. By utilizing NFC ring in e-health authentication, username and password combination can be eliminated and Bluetooth efficiency can be fully utilized in reducing the energy consumption. E-health application is developed by using Eclipse through Android Development Tools (ADT) since it is compatible and flexible with various kinds of mobile phones. Amarino platform is being implemented in this e-health system in order to connect with Arduino IDE processor. Atmega328p can be programmed by using Arduino IDE since it is an integrated development environment for the e-health system development. An Amarino plug in need to be up and running before the e-health application can be executed on the mobile phone. NFC ring control application enables user to do read and write programming. It will enable a user to hold the ring public inlay and put the NFC ring at the best spot on the phone to turn on the Bluetooth module and start the authentication process. At the same time, NFC ring identity will be verified to enhance the security of the EHEART application.

In addition to the implementation of the NFC ring, a secured password less authentication protocol for e-health system has been developed to enhance the efficiency and practicality of the e-health system. There will be four phases which are pre-registration phase, registration phase, login phase and authentication phase. After building up the e-health sensor test bed, e-health authentication protocol will be generated in the e-health base station in order to generate security parameters, master

key and private key. By using EHEART application, user can connect the pulse sensor to mobile device through Bluetooth module and near field communication. After successful authentication between pulse sensor and mobile device, the mobile device will send a login request to the e-health base station. E-health authentication protocol will be implemented and a non-regenerated unique identity for the pulse sensor will be generated through a secure boot process. Based on the existing e-health authentication protocol, data transmission from the patient will go through a third party server first before it is sent to the e-health server or the hospital server. As a result of this situation, it might open the security holes of the e-health system and the system will be exposed to security attacks and privacy issues. Therefore, a secure boot process is done to generate a unique identity for the pulse sensor and to eliminate the role of a third party server in the e-health current architecture.

Confidentiality of the patient data should be the main concern while securing the whole system. The development of the e-health authentication comprises of two main stages which are the generation of the sensor node identity in a trusted platform and the e-health password less authentication protocol. This trusted computing system ensures that it boots and generates only authenticated and genuine code for the non-regenerated sensor node identity. Therefore, a secure boot process will be done first prior to the deployment of the e-health authentication protocol to achieve trusted environment. Each component of the hardware and software for the sensor node has to be validated from the lowest layer to the upper layer. Throughout the secure boot process, a non-regenerated unique identity of the sensor node is produced which will be used as the node identity in the e-health authentication protocol. This unique identity is almost impossible to be cloned or to be regenerated. Thus it protects the whole system from masquerade node cloning attack. This protocol works as a biometric concept where we use human physical features as the unique identity but for a wireless embedded hardware system authentication, a unique identity of the sensor node is generated. Table 1 shows the comparison between the existing authentication protocols and our proposed protocol.

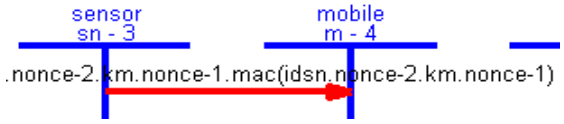

Figure 3. Sensor node to mobile device communication.

Table 1. E-health authentication protocol

Proposed by	Hsiang & Shih (2009)	Sandeep K. Sood (2010)	Hoon-Jae Lee (2012)	Nazhatul Kamarudin (2015)
Username & password	YES	YES	YES	NO
Third-party server	YES	YES	YES	NO
Encrypted data	NO	NO	YES	YES
Unique Identity-based	NO	NO	NO	YES

Development of a secured sensor node is done through a secure boot process to generate the node unique identity. In a secure region of the e-health processor, the data in memory will be unreadable and the secret keys are stored in the secure region of the processor memory. The secure boot process consists of two levels where the pulse sensor unique identity will be generated and verified. The first level of the secure boot process is to analyse the boot loader image and it is assumed non modifiable. The second level of the secure boot process is by measuring the hash value of the first level boot loader image. The pulse sensor node will be able to complete the secure boot process when each level is verified true and then, the unique value generated will be used in the EHEART authentication protocol. The secure boot design considers hexadecimals characters as the comparison value and for validation, hundreds of different images are hashed using SHA-2 algorithm and none of the output can produced an identical eight hashed value in using the same sensor. The unique value from the secure boot process will be used as the pulse sensor identity and to ensure that there will be no other sensor node can generate the same identity. During the secure boot process, it will capture the sensor component identity such as serial number to generate the non-regenerated unique identity of the pulse sensor. Therefore, during the secure boot process of the pulse sensor node, it will generate the unique value (VSN) and capture the sensor component identity to produce non-regenerated sensor node unique identity (IDSN).

After generating a non-regenerated unique identity for the pulse sensor node, passwordless authentication security protocol for mobile e-health will be implemented. Pre-registration phase will be done first where the unique

identity of the pulse sensor is generated through a secure boot process and the unique value will be hashed with the component serial number. Then, during the registration phase, the pulse sensor node unique identity and the mobile device identity will be installed in the e-health base station. The security parameters of the whole system will be installed as well. After that, when the pulse sensor is turned on, the heart rate data from the pulse sensor will be transmitted through Bluetooth communication using NFC ring, and the data is send to the mobile device. The unique identity of the pulse sensor will be verified by the mobile device and if the verification is successful, a login request will be send to the e-health base station in order to continue the authentication process. E-health base station will authenticate the sensor node identity and the mobile device identity in the authentication process. Figure 3 shows the communication from the pulse sensor to the mobile device using security protocol animator.

Mobile e-health authentication protocol is developed using the identity based cryptography algorithms. Details on the authentication protocol can be referred in[32,33]. This authentication protocol will confirm the authenticity of the sensor nodes and mobile device in order to protect the confidentiality and integrity of the data transmitted. By implementing a passwordless authentication security protocol, node cloning and password break attack will not be able to attack the mobile e-health system anymore since the system protocol will authenticate on the unique identity that can only be generated by the trusted sensor node of the user.

3. Result and Discussion

A secure password less authentication using a non- regenerated unique identity and near field communication is proposed to eliminate the third party server. The project results demonstrate the development of a secured passwordless authentication for e-health system. By implementing the near field communication in the e-health system, it can reduce the energy consumption where the Bluetooth module will only be automatically turned on when the mobile device is being touched by the NFC ring. EHEART application does not need any username and password combination for login request and authentication process. Figure 4 shows the e-health prototype with NFC ring and EHEART mobile application.

Figure 4. EHEART prototype for mobile e-health system.

The EHEART application will only be turned on when the authentication is valid and the NFC ring is verified. After the NFC authentication is successful, then the Bluetooth module on the mobile device will turn on automatically and when the application is closed, the Bluetooth connection will be turned off. Therefore, this proposed application can really save the mobile phone battery energy and reduce the energy consumption. Then, the user needs to touch the pulse sensor node in order to monitor their pulse rate data in beat per minute (BPM) and the data will be shown in the EHEART mobile application before the data is transmitted to e-health base station for further analysis or data storage. Figure 5 shows the flow diagram of the EHEART application.

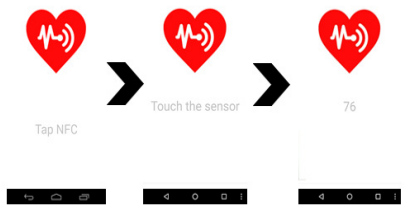

Figure 5. Flow diagram of the EHEART application.

Analysis on the power consumption is done to analyze the feasibility and the efficiency of the EHEART application. The e-health embedded system prototype is analyzed on the power consumption and battery life-time. Analysis on the power consumption of the embedded system has been done and 40.86 miliWatt per hour is used. The analysis of a battery life-time when the embedded e-health system is running concluded that the e-health system can last up to 3 hours non-stop data reading. Comparison of EHEART application with other e-health monitoring application has also be done to evaluate the reliability of the system. Based on the comparison result, EHEART is proved to be reliable and efficient same as other e-health monitoring system. The results of heart rate data reading (BPM) between EHEART and Azumio e-health moni-

toring system are completely similar and precise. Formal analysis on the security protocol is done using model checking tool Automated Validation of Internet Security Protocols and Applications (AVISPA) and Security Protocol Animator (SPAN). It uses a role-based language and programming coding is developed using high-level protocol specification language (HLPSL). The developed model is converted into intermediate format (IF) and then being analyzed by four backend tools which are On-The-Fly-Model-Checker (OFMC), SAT-based Model Checking (SATMC), Constraint Logic Based (Cl-Atse), and TA4SP. The system will verify the proposed protocol and implement Dolev-Yao intruder model to analyse the security attacks on the proposed protocols. Formal analysis on the security protocol is based on the e-health authentication network model discussed before. The authentication system consists of Sensor Node (SN), mobile device (M), and e-health Base Station (BS). The passwordless authentication protocol will verify the unique identity generated by the sensor node during a secure boot process. HLPSL coding is developed to simulate the communication between the pulse sensor, mobile device and the e-health base station. Throughout the formal analysis, it is assumed that before login phase, the unique identity of the pulse sensor has been installed in the e-health server, as well as the mobile device identity. Authentication protocol scheme on the proposed network model is developed where mobile device will check the unique identity of the pulse sensor node in the e-health base station first before decrypting the received data from the sensor node.

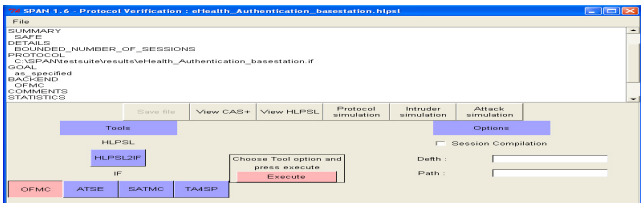

Figure 6. Result on the AVISPA protocol verification analysis.

After successful verification of the pulse sensor node, the e-health base station will receive the login request from the mobile device and then, the base station will authenticate on the mobile device identity. Following the authentication security protocol developed, OFMC and ATSE backend have confirmed the reliability and the functionality of the proposed protocol. This protocol manages to fulfil all three basic security structures which are security, integrity, and confidentiality. Figure 6 below shows the result of the protocol verification and it is proven to be safe from replay attack and node cloning attack.

4. Conclusion

Rapid evolution of wireless technology system together with advancement in wireless sensor network has enabled large development on e-health technology system. The advancement in e-health technology will of course initiate the need and demand for security and privacy in the e-health system network since sensitive data is transmitted throughout the system[34,35]. Moreover, security features in wireless sensor networks will depend on the application needed. Passwordless authentication for e-health monitoring system could replace any electronics health monitoring technology in the future due to its low power consuming, user-friendly and interactive to be used. It can be very helpful in reducing elders discomfort on health monitoring system and assist healthcare unit to monitor patient health in advance without the need to meet the patient in person. EHEART application increases the security and the reliability of mobile e-health monitoring system and enhances the e-health development technology.

5. Acknowledgement

The authors would like to thank Research Management Institute (RMI) of University Technology MARA, members of Information Security and Trusted Infrastructure Laboratory (INSTIL), and Faculty of Electrical Engineering, UITM.

References

1. Mea VD. What is e-health (2): The death of telemedicine? Journal of Medical Internet Research. 2001 Jun; 3(2):1–2.
2. Smith E, Eloff JHP. Security in health-care information systems current trends. International Journal of Medical Informatics. 1998 Oct; 54(1999):39–54.
3. Bahtiyar S, Caglayan M. Trust assessment of security for e-health systems. Journal of Electronic Commerce Research and Application. 2013 Nov; 13(3):164–77.
4. Ambroise N, Boussonnie S, Eckmann A. A smartphone application for chronic disease self-management.

Proceedings of the 1st Conference on Mobile and Information Technologies in Medicine, Prague, Czech Republic; 2013.
5. Chan V, Ray P, Parameswaran N. Mobile e-health monitoring: An agent-based approach. IET Communications; 2008. p. 223–30.
6. Fernández-Alemán JL, Señor IC, Lozoya PÁO, Toval A. Security and privacy in electronic health records: A systematic literature review. Journal on Biomedical Informatics. 2013 Jun; 46(3):541–62.
7. Lou W, Tech V. Secure ad-hoc trust initialization and key management in wireless body area networks. Journal ACM Transaction on Sensor Networks. 2013 Mar; 9(2):1–35.
8. Guo Y, Hu Y, Afzal J, Bai G. Using P2P technology to achieve e-health interoperability. IEEE International Conference on Service System and Service Management (ICSSM); 2011. p. 1–5.
9. Sun Q, Song W, Foundation M. Thinking about some issues of e-health. Journal of China-US Public Administration. 2013 Feb; 10(2):209–16.
10. Thilakanathan D, Chen S, Nepal S, Calvo R, Alem L. A platform for secure monitoring and sharing of generic health data in the cloud. IEEE Future Generation Computer System; 2014. p. 102–13.
11. Desai N, Shahnasser H. A light review of data security and privacy approaches applicable to e-health systems. International Conference on Computing Technology and Information Management; 2014. p. 362–6.
12. Boonyarattaphan A, Bai Y, Chung S. A security framework for e-health service authentication and e-health data transmission. International Symposium on Communications and Information Technology; 2009. p. 1213–18.
13. Bazzani M, Conzon D, Scalera A, Spirito MA, Trainito CI. Enabling the IoT paradigm in e-health solutions through the VIRTUS middleware. IEEE 11th International Conference on Trust, Secuity and Privacy in Computing and Communications; 2012. p. 1954–9.
14. Bai G, Guo Y. Activity theory ontology for knowledge sharing in e-health. IEEE International Forum on Information Technology and Application; 2010. p. 39–43.
15. Ghazizadeh E, Zamani M, Ab Manan J, Alizadeh M. Trusted computing strengthens cloud authentication. The Scientific World Journal; 2014.
16. Zhang R, Liu L. Security models and requirements for healthcare application clouds. IEEE 3rd International Conference Cloud Computing; 2010. p. 268–75.
17. Dong N, Jonker H, Pang J. Challenges in e-health: From enabling to enforcing privacy. International Conference Foundation Health Informatics Engineering System; 2012. p. 195–206.
18. Bai G, Guo Y. A general architecture for developing a sustainable elderly care e-health system. IEEE International Conference On Service System and Service Management (ICSSM); 2011. p. 1–6.
19. Rahim YA, Sahib S, Khanapi M, Ghani A. Pseudonmization techniques for clinical data: Privacys in Sultan Ismail Hospital Johor Bahru. IEEE International Conference on Networked Computing (INC); 2011. p. 74–7.
20. Fengou M, Mantas G, Lymberopoulos D, Komninos N, Fengos S, Lazarou N. A new framework architecture for next generation e-health services. IEEE Journal on Biomedical Health. 2013; 7(1):9–18.
21. Yao W, Chu CH, Li Z. The adoption and implementation of RFID technologies in healthcare: A literature review. Journal on Medical Systems. 2012; 36(6):3507–25.
22. AbuKhousa E, Mohamed N, Al-Jaroodi J. E-health cloud: opportunities and challenges. Journal on Future Internet. 2012; 4(4):621–45.
23. de Souza RL, Lung LC, Custodio RF. Multi-factor authentication in key management systems. 12th IEEE International Conference on Trust, Security, and Privacy in Computing and Communication; 2013. p. 746–52.
24. Jones V, Gay V, Leijdekkers P. Body sensor networks for mobile health monitoring: Experience in Europe and Australia. IEEE International Conference on Digital Society; 2010. p. 204–9.
25. Ghani MKA, Bali RK, Naguib RNG, Marshall IM, and Shibghatullah AS. The design of flexible front end framework for accessing patient health records through short message service. Asia-Pacific Conference on Applied Electromagnetic; 2007. p. 1–5.
26. Martí R. Security in a wireless mobile health care system. International Conference on Emerging application for Wireless and Mobile access; 2005.
27. Zhu X, Han S, Huang PC, Mok AK, Chen D. MBStar: A real-time communication protocol for wireless body area networks. 23rd Euromicro Conference on Real-Time System; 2011. p. 57–66.
28. Fernando JI, Dawson LL. The health information system security threat lifecycle: An informatics theory. International Journal on Medical Informatics. 2009; 78(12):815–26.
29. Gagnon MP, Desmartis M, Labrecque M, Car J, Pagliari C, Pluye P, Fremont P, Gagnon J, Tremblay N, Legare F. Systematic review of factors influencing the adoption of information and communication technologies by healthcare professionals. Journal of Medical System. 2012; 36(1):241–77.
30. Shen P, Liu V, Caelli W. A viable and sustainable key management approach for a national e-health environment. International Conference on e-Health Networking, Applications, and Services; 2012. p. 347–52.

31. Johari AW, Latif M. Tank water level monitoring system using GSM network. International Journal of Computer Science and Information Technologies. 2011; 2(3):1114–15.
32. Kamarudin NH, Yussoff YM, Hashim H. IBE_trust authentication for e-health mobile monitoring system. IEEE Computer Applications and Industrial Electronics (ISCAIE), Langkawi Malaysia; 2015. p. 160–4.
33. Kamarudin NH, Yussoff YM, Hashim H. Two-tier e-health monitoring system. WSEAS Applied Computational Science (ACACOS), Kuala Lumpur, Malaysia; 2014.
34. Thiranant N, Hoon JL. A design of security framework for e-health authentication system using QR code. Advanced Science and Technology Letters. 2013; 38:32–5.
35. Chowdhury N, Bhuiyan MDMH, Samiul I. IoT: Detection of keys, controlling machines and wireless sensing via mesh networking through internet. Global Journal of Researches in Engineering. 2013; 13(13):1–9.