Journal of Computer Science 7 (10): 1465-1473, 2011
ISSN 1549-3636

Ubiquitous Health Monitoring Systems: Addressing Security Concerns

Mahmoud Elkhodr, Seyed Shahrestani and Hon Cheung
School of Computing and Mathematics, College of Health and Science
University of Western Sydney, Australia

Abstract: Problem statement: It is important to secure the transmission of patient's EHR in remote health monitoring systems. Security is among the main issues that need to be realized for the adaption of this monitoring technology. The face of healthcare is changing as ubiquitous computing technologies are being incorporated into the existing infrastructure. We specify the requirements, needed security mechanism, outstanding issues and the future challenges as well as the open problems that need to be achieved. **Approach:** Although there were benefits to technology, approaches that offer reliable privacy and security features must be presented to users in order to make these systems socially accepted. **Results:** We investigated the privacy and security implications generated from the deployment of remote health monitoring technology. To achieve these security requirements, building on the strengths of Transport Layer Security (TLS) protocol, a trust negotiation approach was proposed. The application of this approach results in significant improvements in overcoming security related concerns compared to the traditional identity-based only access control techniques. **Conclusion:** We believe these considerations will eventually contribute toward an efficient and practical deployment of remote monitoring systems.

Key words: Ubiquitous computing, U-health services, monitoring system, healthcare services, remote health monitoring system, security features, Health cast report, community care system, Information Communication Technologies for Health (ICT), Community Aged Care Packages (CACPs)

INTRODUCTION

The healthcare industry is under continuous development and growth. In the 2008-09 financial year, there were 8.1 million patients admitted to hospitals in Australia (A.I.O.H.A. Welfare, 2010). According to the same source, this number reflects an increase of 3.4% on average for each year between 2004 and 2009 for public hospitals and 4.4% for private hospitals. Also, the report states that public hospital recurrent expenditure increased each year by an average of 5.9% between 2004 and 2009. In Europe, a recent report shows that health spending is estimated to increase by 16% in 2020 (Health Cast, 2020). The report further states that e-Health (also written e-Health) industry in Europe was worth approximately 21 billion Euros in 2009. These numbers show the increase in demand on health services. Furthermore, these figures present serious challenges to the maintainability of the current healthcare system and the community care system. Therefore, according to the same report, health Information Communication Technologies for Health (ICT) is presented as a counterbalancing solution to overcome these challenges.

The health ICT industry has the potential for growth in specialized e-Health services such as e-health records, remote monitoring, home and community care. These e-Health services have been scientifically demonstrated to improve the quality of services and result in numerous economic benefits as well. The development of this of technology is associated with a number of factors as described in the taskforce report, for example: Changing patterns of diseases, ageing, increase in demand on community care and remote monitoring services. Ubiquitous health monitoring is one of the applications presented as the future trend of healthcare service.

Ubiquitous health Benefits: The benefits behind deploying health monitoring technology are associated to a number of factors such as, improving the quality of service, reducing medical error, availability of service and to issues related to costs and the problem of constant shortage in medical staff. Community care in Australia,

Corresponding Author: Mahmoud Elkhodr, School of Computing and Mathematics, College of Health and Science University of Western Sydney, Australia

as an example, has been a growing service in aged care for the last two decades, according to a recent report (Welfare, 2009) released by the Australian Institute of Health and Welfare. The report further states that the increase in community care was mainly due to the preference of most people who need support to live at home in the community rather than moving to some form of hospital care. Furthermore, according to the same report, at 30 June 2008 the number of Australian Community Aged Care Packages (CACPs) (Community Aged Care Packages. Available) offered by the government has increased by 57% compared to 2007. While, the number of the recipients of the Australian Extended Aged Care at Home (EACH), 2008 packages has also increased by 29%. Figure 1 below illustrates the increase in demand for home care packages by persons over 70 years of age between the years 1995 and 2008.

In regards to ageing, the European taskforce report states that the number of people over 65 years of age is estimated to increase up to 40% between 2010 and 2030 in Europe. The concerns behind these numbers become clear when we know that people over the age of 65 in Europe receive four times the number of medical tests as others. Consequently, the increase in expenditure on the health sector is associated to the increase of elderly among the population and specifically the cost behind their medical treatment. However, not only ageing has a large effect, but also the changing patterns of diseases, such as in chronic diseases.

Accordingly Yamazaki *et al*. (2009), the authors consider that health monitoring is the fastest growing health service today. They believe that this health monitoring technology, referred to as ubiquitous health (U-health), is developed as a possible solution for monitoring patients at home. Whilst the key issue behind it is to reduce the cost on patients and governments, but with no effect on the quality of services provided. Also, remote diagnostics and patient management technologies have been highlighted as one of the key components of healthcare for the 21st century Weerasinghe (2009). It will also help healthcare providers to react before a current medical condition occurs such as a heart attack or diabetic emergency (Kim *et al*., 2010).

METERIALS AND METHODS

In their study, it was also considered that the homes of the elderly are the best places to collect the medical data and signals related to their body, such as their hearts rate. The authors agree with (Yamazaki *et al*., 2009) that the use of U-health monitoring systems will cut hospital visits and reduce healthcare expenditures.

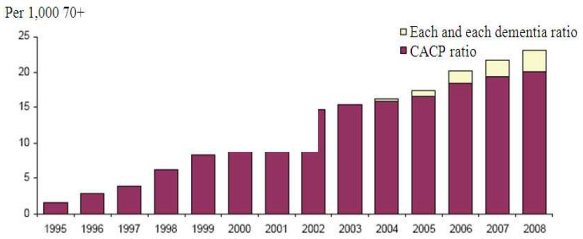

Fig. 1: Ratio of home care packages between years 1995 and 2008. (CACPs and EACH packages per 1,000 persons aged 70 years and over by state/territory and remoteness in PDF)

Other studies such as, Yamazaki *et al*. (2009) (Kim *et al*., 2010; Yao *et al*., 2010) also illustrated on the use of monitoring systems as well. In most of these studies, the system role is to assist and monitor the patients' medical condition by keeping them in their own homes.

Apart from the economic welfares, there are also benefits associated to improving the quality of care and quality of services. Reliability, accessibility, frequency, accuracy and even availability are the sort of quality we refer to. Engdahl, 2009 states that remote health monitoring will be invaluable for people who live in remote locations, or simply those who lack transportation, or are even too ill to visit hospitals easily. In fact, U-health may eventually be less costly than regular visits to hospital. Also, enabling the elderly to stay in their own homes instead of moving to nursing homes is an undisputedly desirable goal.

Ubiquitous health barriers: Although ubiquitous computing is an opportunity for improving the health sector; there are a number of limitations involved. In order for this technology (U-health monitoring technology) to become feasible, a number of challenges are facing its presence. These challenges are related to the deployment of this technology (Lim *et al*., 2010) and to issues such as resource constraints, user mobility, cost, heterogeneity of devices, scalability, security and privacy. While Znati (2005) believes that challenges associated to sensor technology features also exist, such as Quality of Service (QoS), low power consumption and security of the wireless devices.

Therefore, data of a medical nature related to the users (patients) are seen to be very sensitive as they directly concern their bodies and physical integrities. Despite this fact, the users are more and more led to entrust these data to the computer in particular and to the medical system in general. In a U-health monitoring environment the exchange of data will become continuous and incontrollable by default. This is due to

the collected patient's information being transmitted to the hospital for monitoring purposes. A patient holding a device/tag transmitting medical data to the hospital will reveal his or her identity and other personal information as well (Yao *et al*., 2010); such as location information or even his or her name. It is important to note that precise data measuring techniques need to be used as the doctor will recommend treatment based on the analysis of the collected data. Another important consideration is the exposure and exchange of this information is faced with the fear of being intercepted, analyzed or even modified. This process will lead to security and privacy concerns related, but not limited, to the confidentiality of patients and to the integrity of data exchanged. Therefore, due to the sensitive nature of this information, there is an obvious need to secure these data during their collections, transmissions and even their storages.

Yao *et al*. (2010) agree with Lim *et al*. (2010) on the necessity to secure the transmission between RFID tags and the local server. On the other hand, Bluetooth encryption E0 techniques were used for securing the connection between the hub and the mobile device in the study presented Barnickel *et al*. (2010). Other studies, such in (Barnickel *et al*., 2010; Moncrieff *et al*., 2009) regard security and privacy as the right of patients' to decide what, when and to who their information are to be shared with.

The monitoring system: U-health monitoring systems can be referred as 'U-health smart home'. It aims to provide a platform for remote monitoring and assistance to elderly persons at home, such as in (Yamazaki *et al*., 2009). It is an environment of surrounding intelligence. U-health utilizes a range of electronic and terminal computer equipment. Typically, these hardware comprise mobile devices of small sizes, sensors and actuators embedded within the described environment. These devices have the ability to communicate, collaborate and co-operate in an almost transparent manner from users. In the context of a smart home, UC device technologies play a significant role towards the development of a U-health monitoring system. Hence, this system will allow elderly persons to have their medical condition monitored at home by collecting measurements related to their physical body and behaviors. The collected data (measurements) will be transmitted to the healthcare provider for analysis. Consequently, these data are to be examined and directed to the appropriate doctors and specialists. As a result, doctors will have the capability to access the data and perform the necessary required actions, for example, issuing a new prescription. However, the nature of UC provides the possibility to access collected data from various locations and it is not limited to location factors (such as the presence of doctors in hospitals). Therefore, doctors will have access to these data from wherever they have access to an Internet connection. This process allows doctors to have an accurate measurement and precise monitoring of their patients' medical status anywhere and anytime.

Yet, in order to secure the communication between the two end parties (patients and doctors), all sides of the communication held in this environment must be addressed. Thus, the process of collecting data from patients using sensors, transferring it to the hospital and giving doctors ubiquitous access to it, incorporate a number of complex security issues. To achieve this, we divide the environment into phases and analyze the security issues associated. We believe this systematic method of investigation will lead to a better understanding and examination of the security and privacy concerns generated from the deployment of this environment.

Domains A-B-C-D: Domain A - relates to the actual monitoring environment (such as the patient house); where the actual data and measurement are collected from patients. This mechanism is achieved using various ubiquitous computing devices such as sensors and RFID tags.

Domain B: Relates to the mechanism of transmitting the collected data to the healthcare provider (transmission medium) and therefore the generated security and privacy concerns.

Domain C: Relates to the mechanism of storing and analyzing these data. We will be concerned in the issues of access control rights involved and other security aspects such as, when and who have access to data and to what extent.

Domain D: Relates to the mechanism of granting and therefore securing, access to the collected data by a mobile doctor.

For a better understanding, the following scenario is presented:

Alice is a 70 year old woman recovering from a heart attack caused by a sudden variation in blood pressure. After her release from hospital, doctors are in need to monitor Alice's health status. This monitoring process will require precise recording and monitoring of the changes in Alice's blood pressure during any of her normal daily activities in the house. For this purpose, a health monitoring system has been provided to her by the designated healthcare provider. The monitoring system is equipped with tiny sensors and RFID tags.

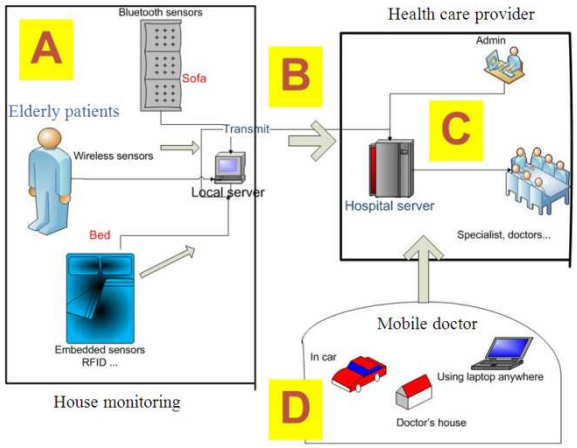

Fig. 2: U-health monitoring system

The aim of these devices is to provide constant observation and measurement of Alice's blood pressure and other physical measurements (Domain A in Fig. 3). The house central server collects data from these sensors and transmits them (Domain B in Fig. 2), every hour, to the hospital server (Domain C in Fig. 2). Next, these data are given to the doctor(s) responsible of Alice's health. A doctor may be present in the hospital or might be somewhere else (Domain D in Fig. 2) accessing these data via the Internet (from his or her home as an example). Further analysis is then taken and in case of emergency, doctors may alert Alice or take whatever action is appropriate.

Kim *et al*. (2010) believe that local server needs to have control over the sensors and devices attached to patients, as when to turn them on or off. Also, they believe that at the lower abstraction level of these functioning devices, these hardware devices need to control and monitor various aspects in the U-health environment. Examples of these aspects are the wearable RFID tags or the sensors planted inside the bed presented in their proposed system. Further, they point that this process of control can be achieved via the sensing and actuating mechanisms of sensors and by the use of RFID mechanism.

Acharya (2010) in his study on security issues in healthcare networks believes that the information collected from various sensors and devices planted in the house should be controlled and accessed via a single access point. While, Lim *et al*. (2010) used a case study which illustrate and analyze the security risks of a wireless body area network for remote health monitoring. In their experiment, devices were embedded inside the body of a patient. The purpose behind this is to monitor the patient's heart rhythm in order to quickly detect any possible sign of a heart attack. They further point out that in these sorts of systems, it is important to have an efficient monitoring and reporting system. Moreover, many wireless monitoring devices used for the transmission of data between sensors and the local server, such as Bluetooth and zigbee, were also proposed in this study Lim *et al*., 2010. However, the authors believed that these technologies weren't developed originally to accommodate real time, high speed and continuous data transfer applications and therefore, further care and work must be done.

Privacy and security concerns: as we have identified earlier, ubiquitous applications (such as sensors and tags) are to be embedded in various devices or appliances and may operate in the background without the users' awareness. Lim *et al*., 2010 see that prior to the real world deployment of the remote healthcare monitoring system, security and privacy risk should be considered and securing the medical data of patients must also be addressed. Further, they state that there is a need to provide users with security and privacy settings into the remote health system before introducing this system to real world. However, the authors acknowledge that it is difficult to develop and provide security features in UC for healthcare monitoring purposes. The reason is due to the limitation of pervasive computing properties, such as the low power consumption of sensors.

RESULTS

As a possible solution, Lim *et al*., 2010 suggest to import cryptographic functions with plug and play gadget that can be used and setup by normal users. For this purpose, Tinyos, ECIES and other cryptographic algorithms were introduced and presented as solutions for securing the communication between sensors. However, the authors concluded that there is a need to perform field testing on these technologies in order to investigate the feasibility of their deployment. On the other hand, the authors proposed also the use of elliptic curve cryptographic algorithm, mutual authentication group and key agreement protocols as a proposed security solution. They also draw attention to the fact that verification of security features in the system must abide to the condition of low power consumption and limited computing resources

Yao *et al*. (2010) agree with Lim *et al*. (2010) on the necessity of securing the connection between the RFID tag and the local database. The authors argue that the benefit of using RFID in medical system settings depends on whether patients are in no doubt that their transmitted medical data will not be misused. Further, they believed that RFID tag associated to patients may

contain private information about them such as name, gender or home address. These types of data should be stored in secured servers due to their sensitive nature. The authors believe that is advisable not to transmit these data over RFID connection, or at least to secure their transmissions. On the other hand, the study emphasizes the importance of telling patients the purpose behind collecting their data. These investigations add an additional concern to the issues of securing the transmission of data between the sensors and the local server - user's consent.

Barnickel *et al*. (2010) detailed security and privacy related to the implementation of the health net system is presented. This system is described as a mobile electronic health monitoring system. The study demonstrated that systems intended for monitoring purposes are becoming more feasible. This feasibility was associated to the rapid development of 3G networks and to the fall in their costs. Furthermore, it pointed at two telemonitoring systems based on 3G technologies which have already been completed for testing. The first one is the Australian personal health health monitoring (Gay, 2010); which achieves some privacy settings, but does not provide any detailed security specification. While the second one is the European (MobiHealth, 2004); which the authors consider as not having any privacy features at all. Other commercial systems were also described as not having clear security and privacy specifications. Therefore, it is concluded in this study that precise security and privacy specification are required. To overcome this shortcoming, they present a system which uses the following devices: Sensor node, hub (which collects data from sensors) and a mobile device. Security during data collection between the sensor node and the hub was achieved using Zigbee AES-128 encryption techniques.

DISCUSSION

Security and privacy implications were analyzed in the study presented by Kargl *et al*., 2008 on E-health monitoring. The authors discussed the types of threats and attacks that are likely to occur when considering ubiquitous health monitoring system.

Based on the type of attacks discussed above, a list of the type of attackers and their origin is given below:

- External passive attacker: Is when an attacker eavesdrops on the communication without the ability to interfere
- External active attacker: Is when the same attacker has the ability to modify or forge packets
- Internal passive or active attacker: The attacker in this case is part of the environment and has physical access to the devices. Their influence varies from accessing the data to actively modifying and falsifying part of it or turning the devices off

We assume both internal and external attacks may occur on the sensors and other target components of the system. Attacking these devices may vary from recording the data up to modifying it. While internal attack supposes that the attacker has an actual access to the devices. While the second assume that an attacker can intercept the communication between the home server and the hospital server. Therefore, based on this interpretation, we present the following security requirements:

- Connection between sensors and the local server must be secure
- Data exchanged shall not reveal any personal information or identity (we believe there is no need to exchange personal information between sensors and local server. Therefore, only medical data and measurement are to be transmitted. However, there is a need to identify the source of these data at the server side, while ensuring anonymity is preserved)
- Integrity protection during transit must be used (to ensure that the system is able to recognize false and unoriginal data)
- Problem of availability must be addressed and the system should not be designed in a single point of failure architecture

While, Acharya (2010) noted the need to protect the medical data at all time (during transmission and storage). Hong *et al.* (2004) analyzed the privacy risk encountering the use of pervasive computing. To help categorize and split the problems presented Inseop *et al.* (2006), the authors divided the privacy risks into a set of questions. Therefore, the questions related to Domain B are summarized below: Is there the potential for malicious data observers? If yes:

- What kinds of personal information are they interested in
- How is personal information shared
- What is the quality of the information shared
- What kinds of personal information are shared

Marx (2001) analyzed the privacy risk by categorizing it into different types of identities that need to be protected. Thus according to Marx, intercepting the communication must not reveal the following:

- A person's address, name and other direct personal data
- His unique identifier such as bank account number, driver license number
- Pseudonym that can be easily traced.
- Person behavior, food style, dressing style
- Person social characteristics such as sexual orientation or type of employment
- Personal relationships

Barnickel *et al*., 2010 in addressing the security aspects of the communication held between a mobile device and another (in their case, communication held between mobile devices are similar to the communication held between the local and the hospital server) proposed the use of AES-128 encryption techniques. Further, a message authentication code is to be used on the application protocol; while session key agreement and authentication protection techniques are to be used for securing the transmission over wireless LAN.

The investigation and the analyses made in this work lead to the following results: (1) There is a need to secure the connection between the two servers in a way that no data can be revealed and no data mining can be possible if the transmission were intercepted and (2) there is a need to protect the patients' personal data in a way that no personal data are to be exchanged or in some cases, as in the studies reviewed before, the user chooses what kind of personal data is to be exchanged. Consequently, our interpretation lies on the following statement: The security and the privacy risks depend on whether the data being intercepted discloses private information related to the patient or not. That is, if data cannot be traced back to the user and does not include any elements which reveal any of the user identities (Marx, 2001) the data being intercepted and hacked is of no threat on users.

To overcome some of the security requirements identified in this work we propose and approach in which we refer at trust negotiation. The aim of the proposed approach is to secure remote access to patients' Electronic Health Records (EHR) over a public network. It builds on the strengths of TLS as the underlying protocol. In a remote monitoring system designed for monitoring elderly persons, the protocol provides healthcare professionals with secure remote access to the patient's EHR and also secures the transmission of patients' EHR between the healthcare provider's server and the healthcare professional's mobile device over the Internet. It works by establishing a secure session between the healthcare professional's device and the healthcare provider's server. The healthcare server is where the patient's EHR is actually stored. This session is created using the TLS handshake mechanism. The TLS session is used to ensure the encryption of the exchanged messages and protection against intruders. After establishing the secure session, three conditions must first be made before the release of any sensitive data:

- Authenticating the healthcare professional
- Authenticating the device in use
- Authenticating the environment of access and the person receiving healthcare

These are the requirements necessary to identify the players involved in a single healthcare transaction. This includes (1) the person administering healthcare (the healthcare professional), (2) the device in use by the healthcare professional, (3) the person receiving healthcare and the place where healthcare occurs. Thus, these three levels of authentication must be achieved before granting healthcare professionals any access to patient's EHR.

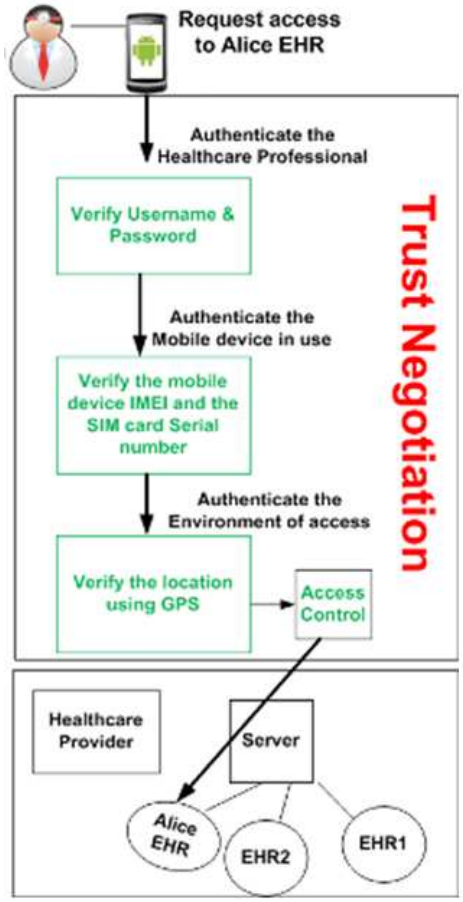

Fig. 3: Trust negotiations

In an elderly remote monitoring system, a Healthcare Professional (HP) represents the person administering healthcare who may visit the house of the elderly; which is the location where healthcare occurs, to conduct a medical examination, regular check up or other required healthcare activities. There is a need for these healthcare professionals to remotely access the elderly' Electronic Health Records. The reason of accessing the EHR can vary from reading the data history to modifying or adding new data to the records. Healthcare professionals will use their mobile devices, as an example, to remotely access the EHR. This will lead to security, authentication and access control issues, such as access rights policies, authorization and authentication. Concerns about the confidentiality and the privacy of the elderly are also raised.

The trust negotiation approach was implemented as part of a mobile application which runs on the Android operating system, as shown in Figure 4. The application (the App) is modeled in terms of a client and server architecture wherein a client requests information from a server. The server typically responds with the requested information. Implementing trust negotiation on the server required the implementation of a server API. This API acts as a web service. It has the responsibility of handling incoming messages from the client and outgoing messages from the server. This is achieved by using the HTTP request methods. Therefore, the API re-uses the messages and the methods already defined in the HTTP protocol, such as the method HTTP Post. For instance, this method is used to send the username and password of the healthcare professional, the mobile IMIE and the SIM serial numbers as well as the location parameters (the GPS longitude and latitude) to the server. The server API also has the responsibility of reading and parsing the client's message and responding accordingly.

Fig. 4: The application screen shot

To remotely access the EHR of a particular monitored person, the healthcare professionals use the App installed on their Android mobile devices and enter their usernames and passwords to logon to the App. Subsequently, the App carries out, in a transparent manner to the healthcare professional, the trust negotiation process; which involves the three levels of authentication previously described. It silently performs the authentication process within a secure session. This guarantees the encryption of the messages exchanged between the client and the server. If trust negotiation succeeds and the healthcare professional had sufficient rights to access the requested EHR, then access to this particular monitored person's EHR will be granted. This application was tested to be fully functional running on an Android mobile device emulator. It can be installed on a wide range of mobile devices which run Android as an operating system, such as, HTC Desire. Also, it operates on wireless connections, such as, WI-FI or over 3 and 4G Mobile Networks. This application has demonstrated the successful integration of trust negotiation and the TLS protocol. These experimental works confirm that by applying the proposed trust negotiation approach, the expected analysis results can be achieved. The developed application is also practical and easy to adopt, as users are not required to have any additional knowledge or expertise in the use of the underlying technologies. The results collected from this experiment showed significant improvements in overcoming security related concerns compared to the traditional identity-based only access control techniques. The improvements in the security of the remote monitoring systems are achieved by providing extra protective features to the access control and authorization process before the release of any data over unsecured network.

CONCLUSION

The research presented in this document call for the need to incorporate end-to-end interconnection security features in a U-health monitoring system. Future research must be concerned in analyzing the issues related to end-to-end integrity, confidentiality of information flow and the protection mechanisms applied for the transmission, processing and storage of Electronic Health Record (EHR) and personal data, as illustrated in this study. They must aim to ensure that mining, modification and eavesdropping on data will not be possible. It is hoped that consideration and evaluation of such security issues will ultimately result in improving the effectiveness of the system and the

early deployment of this technology. The approaches proposed in this study ensure that patients' EHRs are only disclosed to the authorized healthcare professional, on the registered device and at the appropriate locations. They ensure the confidentiality of information, by securing its transmission, using Transport Layer Security (TLS) as the underlying protocol. Building on the strengths of this protocol, a trust negotiation approach is developed. This approach authenticates the person receiving the care, the person administering it, the mobile device used in accessing the health information, as well as the location where the healthcare is administered.

REFERENCES

Acharya, D., 2010. Security in Pervasive Health Care Networks. Proceeding of 11th International Conference on Mobile Data Management (MDM), May 23-26, IEEE Xplore Press, USA, pp: 305-306. DOI: 10.1109/MDM.2010.38

AGDHA, 2011., Community Aged Care Packages. Australian Government Department of Health Ageing. http://www.agedcareaustralia.gov.au/internet/agedcare/publishing.nsf/content/CACP-1

AIHW, 2009. Aged care packages in the community 2007-08. Australian Institute of Health and Welfare.

AIHW, 2010. Australian hospital statistics 2008-09. Australian Institute of Health and Welfare.

Barnickel, J., H. Karahan and U. Meyer, 2010. Security and privacy for mobile electronic health monitoring and recording systems. Proceeding of IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks (WoWMoM), June 14-17, IEEE Xplore Press, Montreal, QC, Canada, pp: 1-6. DOI: 10.1109/WOWMOM.2010.5534981

Engdahl, S., 2009. Stewards of the Flame. 1st Edn., Sylvia Engdahl, Eugene, ISBN: 0615314872, pp: 498

Health Cast, 2020. Creating a Sustainable Future," PricewaterhouseCoopers' Health Research Institute.

Hong, J.I., J.D. Ng, S. Lederer and J.A. Landay, 2004. Privacy risk models for designing privacy-sensitive ubiquitous computing systems presented at the Proceedings of the 5th conference on Designing interactive systems: Processes, Practices, Methods and Techniques, (DIS, 2004) ACM New York, USA, pp: 91-100. DOI: 10.1145/1013115.1013129

Inseop, K., L. Byunggil and K. Howon, 2006. Privacy-friendly mobile RFID reader protocol design based on trusted agent and PKI in consumer electronics. Proceeding of IEEE 10th International Symposium on Consumer Electronics, (ISCE, 2006), IEEE Xplore Press, St. Petersburg, pp: 1-6. DOI: 10.1109/ISCE.2006.1689530

Kargl, F., E. Lawrence, M. Fischer and L. Yen Yang, 2008. Security, privacy and legal issues in pervasive ehealth monitoring systems. Proceeding of 7th International Conference on Mobile Business, ICMB, July 7-8, IEEE Xplore Press, USA, pp: 296-304. DOI: 10.1109/ICMB.2008.31

Kim, Jin; Choi, Hyeok-soo; Wang, Hui; Agoulmine, Nazim; Deerv, M. Jamal; Hong, James Won-Ki; , 2010. POSTECH's U-health smart home for elderly monitoring and support. Proceeding of IEEE International Symposium on World of Wireless Mobile and Multimedia Networks (WOWMOM). June 14-17, IEEE Xplore Press, Montreal, QC, Canada, pp: 1-6. DOI: 10.1109/WOWMOM.2010.5534977

Lim, S., T.H. Oh, Y.B. Choi and T. Lakshman, 2010. Security issues on wireless body area network for remote healthcare monitoring in Sensor Networks. proceeding of IEEE International Conference on Ubiquitous and Trustworthy Computing (SUTC), June 7-9, IEEE Computer Society Washington, DC, USA, pp: 327-332. DOI: 10.1109/SUTC.2010.61

Marx, G.T. 2001. Identity and Anonymity. Some Conceptual Distinctions and Issues for Research In: Documenting individual identity: the development of state practices in the modern world, Caplan, J. and J.C. Torpey, (Eds.)., Princeton University Press, Princeton ISBN: 0691009120, pp: 311-344.

Moncrieff, S., S. Venkatesh and G. West, 2009. A Framework for the design of privacy preserving pervasive healthcare. Proceeding of IEEE International Conference on Multimedia and Expo, ICME, June 28-3, IEEE Xplore Press, New York, pp: 1696-1699. DOI: 10.1109/ICME.2009.5202847

Weerasinghe , D., 2009. Electronic Healthcare First International Conference, eHealth 2008. 1st Edn., Springer Link, Springer, pp: 222. ISBN3642004121, 9783642004124

Yamazaki, A. A. Koyama, J. Arai and L. Barolli, 2009. Design and implementation of a ubiquitous health monitoring system. Int. J. Web. Grid. Serv., 5: 339-355. DOI: 10.1504/IJWGS.2009.030263

Yao, W., C.H. Chu and Z. Li, 2010. The use of RFID in healthcare benefits and barriers. proceeding of IEEE International Conference on RFID-technology and applications (RFID-TA), June 17-19, IEEE Xplore Press, Guangzhou, pp: 128-134. DOI: 10.1109/RFID-TA.2010.5529874

Znati, T., 2005. On the challenges and opportunities of pervasive and ubiquitous computing in health care in pervasive computing and communications. Per Com. Proceeding of the 3rd IEEE International Conference on, March 8-12, IEEE Xplore Press, USA., pp: 396-396.