Security and Privacy Framework for Ubiquitous Healthcare IoT Devices

Ebrahim AL Alkeem, Chan Yeob Yeun, M. Jamal Zemerly

Khalifa University, Electrical and Computer Engineering Department,
PO Box 127788, Abu Dhabi, UAE
ebrahim.alzaabi@kustar.ac.ae, cyeun@kustar.ac.ae, jamal.zemerly@kustar.ac.ae

Abstract— **With the support of the wearable devices, healthcare services started a new phase in serving patients need. The new technology adds more facilities and luxury to the healthcare services, Also changes patients' lifestyles from the traditional way of monitoring to the remote home monitoring. Such new approach faces many challenges related to security as sensitive data get transferred through different type of channels. They are four main dimensions in terms of security scope such as trusted sensing, computation, communication, privacy and digital forensics. In this paper we will try to focus on the security challenges of the wearable devices and IoT and their advantages in healthcare sectors**

Key words: Security, Privacy, WSN, IoT, WBANs, RBAC

I. Introduction

Wearable devices are being used in a wide range of applications area, the major application domains are related to healthcare, in terms of monitoring, controls and authentications. The use of such devices can be very helpful in attending to patients daily activities. Wearable devices came to change healthcare culture in terms of patient monitoring and managing their health status. Also they become so trending in handling sensitive surgeries. Wearable devices become a need in healthcare sectors due to the benefits that they can reflect.

The UAE is ranked second highest worldwide for diabetes prevalence. About 19.5% of the population is currently living with diabetes according to statistics released by the Imperial College London Diabetes Centre [1]. Figure 1 shows which age group in the population have the highest proportions of diabetes.

The top line explains the distribution of diabetes prevalence by age for the UAE, the dotted line reflects the world distribution of diabetes prevalence by age. However, the middle line shows the MENA region of diabetes prevalence.

Many middle and low-income countries have more people under the age of 60 with diabetes compared to the world average. Meanwhile, for high-income countries, a growing population over the age of 60 makes up the largest proportion of diabetes prevalence. The need of IoT devices came through the severe requirements of the UAE healthcare sector due to the huge number of patients that suffer from diabetes and high blood pressure.

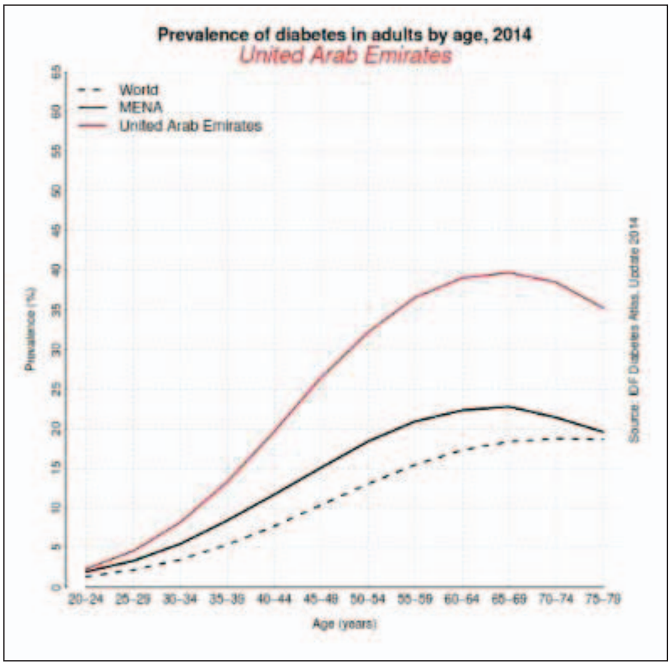

Figure 1: UAE Vs World prevalence of diabetes [1].

We started collaboration with Dubai Health Authority (DHA) in terms of securing medical records as they are in the process of converting all medical records electronically in order to provide security and privacy to patients' records.

IoT devices were developed for healthcare services based on Wireless Sensor Network (WSN) [2]. It can be used to measure patients' conditions through generating clinical data and transmit to a repository or a service for healthcare via wireless network infrastructure [3].

978-1-908320-52/0/$31.00 ©2015 IEEE

The collected medical data through the WSN can be transmitted to a remote server or stored locally in the internal memory of the wearable devices. However, there are many security challenges that can be obstacles to their widespread use such as memory capacity of the wearable device and man in the middle (MITM) attack.

Wearable devices can carry sensitive data about the patients as they will carry many critical data that should be kept secret due to many reasons. Health insurance portability and accountability act of health care records states the obligation to protect the healthcare information.

The need of securing such information from MITM attack came for protecting such important information about the patient which can be legally or socially critical. In our opinion such data needs to be kept secret or encrypted in order to enhance secure transmission of wearable device data. Therefore we recommend encrypting the data before transmitting it to the remote server by using one of the encryption algorithms such as Advance Encryption Standard (AES) [4].

Security challenges require the developments of a number of new versions of platforms and technologies including devices and process identification. In order to reduce the attack possibilities, the potential of the malicious attacks can be moved from the internet to the physical world. In other words malicious people can attack the physical devices coming through the transmission channels from the internet. Therefore, it is highly recommended to allow multiple layers to be present once it comes to IoT security.

The abstraction levels range from physical layers of sensors, computation and communication. The semantic layers work on collecting all sensitive data which can be easily entrapped by the attacker and cause huge damage in the software level as they cover a large number of devices and processes. The majority of the IoT devices can operate on the passive mode without batteries. As their energy can be harvested or received using a wireless medium. The advantage of using passive mode can be reflected in very low area and energy requirements, more resilient against side channel and physical attacks and enable creation of secure and trusted information flows [5].

In the near future most of the devices will be part of the IoT ecosystem; each of them will have a unique identifier similar to the IP address, which will allow easy tracking of the data flow. User information can be gathered from different wearable devices and fed into a main server which get stored and processed. As an example a user can use a number of wearable devices such as blood pressure sensor, sugar level sensor and etc. All data get transmitted to the main server which can be difficult privacy task as attacker can integrate information from different sets and modalities at the semantic level. Combining different data from different sources of information at the semantic level can result in extracting of unexpected data.

Our main motivation is to ensure that the majority of the security contributions will be tackled by applying the proposed framework which overcomes the most security requirements along with the privacy issues.

The overall structure of this paper consists of a brief introduction about the IoT devices followed by the current state-of-the-art, Section III explains the use of the wearable system in healthcare. Section IV lists the healthcare security challenges. In Section V we present the proposed framework. Finally, Section VI represents the security analysis of the proposed framework and will be followed by the conclusion.

II. Current State of the Art

Wearable devices usually come in sensor format which can be small in size to practically be used by the end user also to reduce the energy consumption. When size and energy consumption is in place we need to think about a technology that requires less energy than those currently used. Near field communication (NFC) can be active in such areas. As people are looking for a technology with less power consumption and minimum cost.

The main characteristic of NFC/RFID is that it is a wireless communication interface with a working distance limited to about 10 cm. The need of NFC/RFID security becomes important by increasing the number of applications that supports it. NFC can be used in many useful fields [6, 7]. Many people are using NFC technology in their daily activity as it can be used for money transactions, downloading applications and so. On NFC/RFID protocol is an efficient technology that comes with major security challenges. The security of mobile transactions is not an easy subject after looking at the characteristics of this system [8, 9].

A. *Secure key management scheme*

The need of a secure system to handle key management or key exchange based on Elliptic Curve Cryptography (ECC). It is a secure key management exchange which can help in exchanging keys efficiently to protect patients' medical information in healthcare system. ECC can be divided into three main phases as setup, registration, verification and key exchange [10]. The system can work in identifying the user through the identification code which SIM card number in a patient's smart phone with the private key generated by the legal use instead of the third party. This leads to preventing replay attack. Also the counter number can be helpful for each authenticated message in order to provide resistance to replay attack.

B. *Security requirements in WBANs*

The security issues in networks are always top priority as they are concerned of transferring sensitive patients' data and acting as channel. Wireless body area networks (WBANs) been devolved to overcome the following attacks [11]:

1) Eavesdropping: Attacker can eavesdrop packets from node to node as the wireless channel in WBANs is open. This allows attackers to intercept data, and help them to obtain sensitive and valuable information about the patients. We can solve such issue by

applying cryptography techniques to our framework in order to overcome this attack.

2) Data modification: Attackers try to replace the information or modify it with minor changes, the modified data sent back to the receiver to achieve some illegal activities. In this case we can secure our proposed framework by applying hash functions.

3) Replay Attack: A part of the valid information can be sent back by the attacker to the original receiver after some time to achieve same purpose in a different case. We can avoid such attackers' behaviours by applying nonce to the messages.

4) Denial of service: Attackers try to flood the system with traffic that is higher than system capacity. In this case we can attach a strong firewall, IDS, and IPS to filter such attacker behaviours.

5) Man in the middle attack (MITM): It is the type of attack where the attacker positions himself between two parties and gains access to data that the two parties were trying to send each other.

In order to minimise security threats on the communication channel we need to ensure the following:

1) Access control: It works in enforcing different access rights for different users. Data should be classified based on the sensitivity and each user will have different access level. As an example a doctor will have more data access than a nurse. Access control can also cover the command/instructions/query from an external user.

2) Authentication: This part is important to allow right people to access the right data. Each message needs to be authenticated before sending it. The external user needs to establish authentication process to allow smooth access. Mutual authentication will be the most convenient solution to overcome such attacks.

3) Unforgeability: Body area network (BAN) controller creates a signed and encrypted text to device legal external users. An efficient security mechanism must be properly defined against masquerading attacks [12].

III. Use of wearable devices in healthcare

Wearable devices are meant to add technologies in everyday life, in order to make human life easier and allow smooth data exchange. Wearable devices can be present in many areas such as health, sports, entertainment, and security industry. Figure 2 explains the healthcare system architecture:

Doctors can use wearable devices to monitor their patients remotely. These devices consist of three building blocks:

1) Sensing and data collection hardware to collect physiological and movement data.

2) The communication hardware and software to relay data to a remote center.

3) The data analysis techniques to extract clinically-relevant information from physiological and movement data [13].

The wearable devices depend on their local memory which stores the gathered information about the user. Due to capacity limitations, short range connectivity has been introduced such as Bluetooth and NFC. Recent researchers have focused on improving the connectivity range of the wearable devices using more powerful devices such as mobile phones or tablets. These intermediate devices open up new security challenges. As some of them can be malicious and try to intercept or modify the information in transit during wearable devices communications. As it gets connected to the internet, attackers target them to access or modify the data.

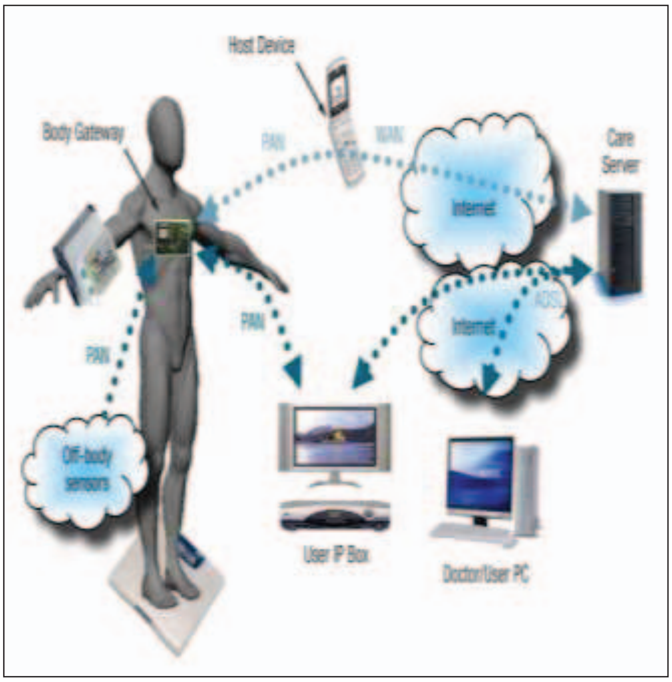

Figure 2: Healthcare system architecture [14]

Wearable devices can be used and developed in a surgical practice in three main roles: assistance, augmentation, and assessment.

Assistance explains the physical tasks that can be replaced by the wearable device in surgical practice, which reflects in different type of tasks. Such as the use of an arm-mounted device to allow gesture control of a PACS system to allow synchronized review of cross-sectional imaging at the time of surgery without breaking sterility [15].

Augmentation works for real-time monitoring of the information to the surgeon during clinical or surgical encounters. The data can take different format as example device data, static reference material, biometric data, and live communication with colleagues or others.

Hospitals use assessment in measuring performance and outcomes which can be used in surgical education. An example of outcomes measurement would be the tracking of breathing and sleep in patients before and after surgery to correct a deviated septum.

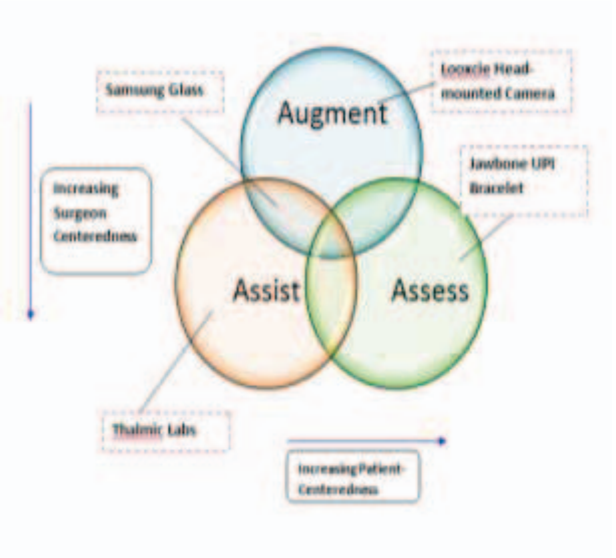
Samsung Glass
Looxcie Head-mounted Camera
Augment
Jawbone UPI Bracelet
Increasing Surgeon Centeredness
Assist
Assess
Thalmic Labs
Increasing Patient-Centeredness

Figure 3: Wearable technology functions within surgical practice

In this paper, we will focus on the wearable devices that can be used in the healthcare sector.

IV. Healthcare Security challenges

Many requirements areas for wearable devices in order to solve the security challenges that can affect exchanging information with other devices or services [16].

Wearable device faces many challenges in term of security such as Replay attacks, MITM attacks, modification and masquerading attacks. Replay attack can be taken care of by introducing time stamp or nonce to the system as it will be valid for a period of time. Masquerading attacks occur when the attacker pretend to be an authorized user to gain greater privilege than what they are authorized for. We can eliminate the effect of such attacks by introducing two factor authentications as example: biometric with token. The authentication part in the wearable devices faces many challenges in terms of the ability of exchanging information between other devices or services. The size limitation of the wearable device and memory capacity is the major concern that is why we need to transmit the data through an intermediate device to allow more flexibility in terms of usage. The authentication part needs to be addressed wisely to be able to transfer the information securely. Also a secure imprinting mechanism needs to be considered to allow the wearable device to differentiate between trusted and untrusted intermediate devices. It is important for the wearable devices to differentiate between the trusted users and the attackers.

The wearable device user needs to authenticate him/herself through a strong authentication credentials (password, certificates, etc.) to minimise the credentials sniffing possibility by an intruder. Also he/she can combine two types of credentials or more in order to increase the level of security as an example a user can use two or three credentials in order to authenticate him/herself, he/she for example, can use password, certificate and biometrics. Two or all of them depend on the criticality of the data. Wearable devices can implement encryption algorithm and encrypt all the data transmitted from the wearable devices and get decrypted in the intermediate devices.

V. Proposed Framework

In this part we will propose three different security levels depending on the sensors location on the wearable system. As we know that the wearable system consists of three main parts: 1) Wearable sensors such as Samsung glass, sugar level sensors, etc. 2) Intermediate devices such as mobile phones or iPADs. 3) Remote server to be able to store patients' record and share it once it is required. Figure 4 shows the main scheme elements.

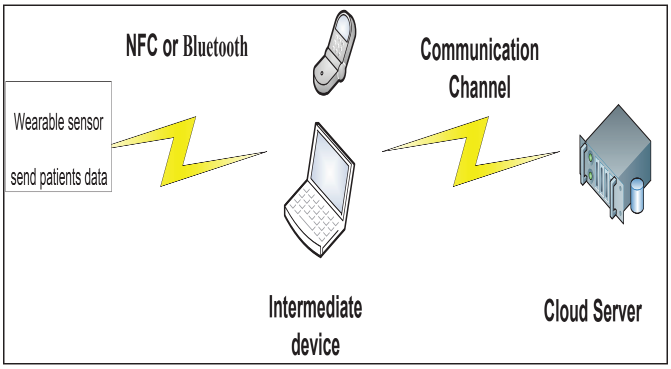

Figure 4: Wearable system elements

Once the patients use a wearable device which measures body activities and converts the body signals to values in order to be understood by a human, such information needs to be classified. Data can be classified depending on the classification matrix that can be used in Public, Restricted, and Secret. We can use the suitable level of security depending on the criticality of the information being sent and type of the patients which can be reflected by the classification matrix. The unclassified data or the public one will not require high security process as it can be available for public. In this case we can use an untrusted intermediate device (no authentication is required). The data which is classified as restricted we can apply intermediate security level such as mutual authentication and exact location of patients [17].

Finally the data which is classified as secret needs to be treated with high security level as it needs to use secure pairing and mutual authentication. The authentication part can be achieved using a PIN code with a biometric token. After a successful authentication, role base access control (RBAC) can be considered in which permissions are associated with roles, and users made members of certain roles [17]. For example, it allows doctors to access the authorized patient data as per the designed roles. By applying both authentications and RBAC to the wearable healthcare system, we can ensure security for patients' data records.

978-1-908320-52/0/$31.00 ©2015 IEEE

VI. Security analysis of the proposed Framework

The following flowchart explains the patient data flow and how it connect to different nodes that can act automatically in case of an emergency

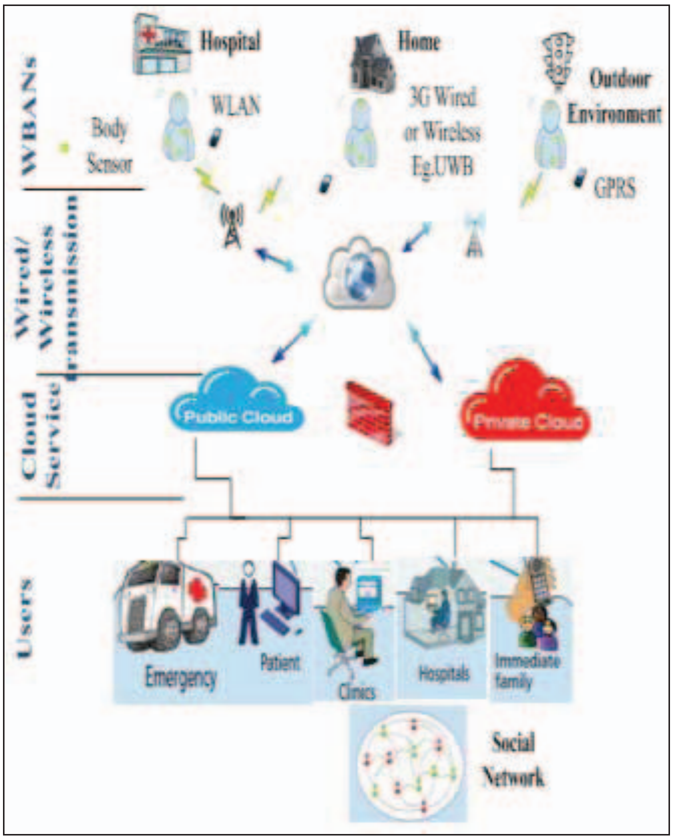

Figure 5: A Framework of healthcare system.

This efficient model can minimize both operation time and cost, as it reduces the human interaction in the operation part as patients will be more self dependent and can be monitored remotely through the wearable sensors. The information will be sent to the main server through the different channels, as explained in Figure 4, which can be used later by other users. Patients' data get updated automatically and fed to the cloud server as Figure 5 shows. Therefore there is no need for the nurse to report patients' health status as they can go anywhere and enjoy their life. From Figure 5 we can notice that the proposed framework consists of four main parts, WBANs, wired/Wireless transmission, Cloud service, and Users. Each part pretends to function according to their area of speciality.

The WBANs in the proposed framework show three situations that the patient can be in and how the data can be sent through wired/wireless transmission. Patients can enjoy their life regardless of their location or whether they are in the hospital or outside; their data will be transmitted through different wired/ wireless technology as Figure 5 shows.

The need of the cloud service occurred due to the huge number of data that get transmitted from the healthcare sensors applications and the limitations of the internal data memory of the wearable devices. The Mobile cloud computing (MCC) which has been used in the proposed framework is generally becoming a promising technology due to the flexibility in computing massive storage, and software services in a scalable and virtualized manner at low cost.

MCC provides extra features to the healthcare system as it provides cost effective, scalable, and data- driven pervasive healthcare system which must be able to realize long-term health monitoring and data analysis of patients in different environments. In this framework we used a hybrid cloud computing of private and public which can accelerate the migration from existing IT resources in the hospitals to cloud computing, make full use of WBAN resources, and reduce costs. The hybrid cloud can be effective once privacy is considered and RBAC is activated. We introduced the social network to this framework due to the important role of such network in increasing the awareness across the public. Also, this is useful to provide analysis modelling of patient communication and education. The proposed framework is a smart approach which minimizes the human interaction and gives patients more flexibility. As the server connected to the main parties (emergency, doctors, and family) can help or monitor their status, patients can enjoy their life with no worry about the nearest hospital that they can go in case of an emergency.

VII. Conclusion

Healthcare systems are facing many challenges in term of security due to the increase in the number of the wearable devices and their applications as they have easy access to sensitive data about the patients. Patients' data needs to be kept secret due to many reasons. Attackers try to gain access through these new technologies seeking sensitive data that can be used illegally against patients. The new proposed scheme focuses on two main parts authentication and role base access control. The need of such security service will enhance the security levels of such technologies and increase the quality of healthcare services. Such approach needs to be considered wisely as we are dealing with sensitive patients data that any preach or leak of it will lead into lack of trust or misuse. The proposed scheme allows secure monitoring of patient conditions after leaving the hospital. As patients will stay connected remotely with the main server and will be attended to once needed.

Future work will focus on compiling the private cloud network security with the proposed frame work in order to enhance the security of the healthcare system. Furthermore, we will develop a secure healthcare system that can securely connect the IoT devices with the private cloud. Another important issue worth investigating is determining and verifying the authentication of the health care data in the private cloud. Although the existing privacy preserving mechanisms offer support to maintain the authentication of data in the cloud. A simulation of a real data can address the missing gaps.

REFERENCES

[1] C. K Hwang, P. V. Han, A. Zabetian, M. K. Ali, K. M. Narayan, "Rural diabetes prevalence quintuples over twenty-five years in low and middle-income countries: a systematic review and meta-analysis", Diabetes Research Clinical Practice, Vol. 96, No.3, pp.271-285, 2012.

[2] S. M. Metev and V. P. Veiko, *Laser Assisted Microtechnology*, 2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag, 1998.

[3] J. Hui, D. Culler, and S. Chakrabarti, "6LoWPAN: Incorporating IEEE 802.15. 4 into the IP architecture–internet protocol for smart objects (IPSO) alliance, white paper #3," 2009.

[4] J. H. Kong, L.-M. Ang, and K. P. Seng, "Minimalist security and privacy schemes based on enhanced AES for integrated WISP sensor networks," *Journal of Communication Networks and Distributed Systems*, vol. 11, no. 2, pp. 214–232, 2013.

[5] A. Dunkels and J. Vasseur, "IP for smart objects, internet protocol for smart objects (IPSO) alliance, white paper #1," 2008.

[6] J. R. Smith, K. P. Fishkin, B. Jiang, A. Mamishev, M. Philipose, A. D. Rea, S. Roy, K. Sundara-Rajan, "RFID-based techniques for human-activity detection," *Communications of the ACM*, vol. 48, no. 9, pp. 39–44, 2005.

[7] K. Rowe, "Securing microcontroller RTOSes for the internet of things, "http://www.embedded.com/design/operating-systems/4429868/Secur-ing -microcontroller-RTOSes-for-the-Internet-of-Things, 2014.

[8] M. A. Shemaili, C. Y. Yeun, K. Mubarak and M. J. Zemerly, "A New Lightweight Hybrid Cryptographic Algorithm for The Internet of Things", In Proceeding of the International Conference for Internet Technology and Secured Transactions (ICITST'12), pp. 87-92, 10-12 December, 2012, London, UK.

[9] N. W. Lo, Kuo-Hui Yeh and C. Y. Yeun, "New Mutual Agreement Protocol to Secure Mobile RFID-Enabled Devices", Information Security Technical Report, Elsevier, Vol. 13, No. 3, pp. 151-157, August 2008.

[10] K. Han, C. Y. Yeun, T. Shon, J. Park and K. Kim, "A scalable and efficient key escrow model for lawful interception of IDBC-based secure communication", International Journal of Communication Systems, Wiley, Vol. 24, No. 4, pp. 461-472, April 2011.

[11] M. Potkonjak, S. Meguerdichian, and J. L. Wong, "Trusted sensors and remote sensing," in *IEEE Sensors*, pp. 1104–1107, 2010.

[12] Y. Tang., "CleanOS: Limiting mobile data exposure with idle eviction", in *Operating Systems Design and Implementation (OSDI)*, vol. 12, pp. 77–91, 2012.

[13] O Gul, M. Al-Qutayri, Q. H, Vu and C. Y. Yeun, "Framework of a National Level Electronic Health Record System", In Proceedings of the International Conference on Cloud Computing Technologies, Applications and Management (ICCCTAM), Dubai, UAE, 8-10 December, 2012.

[14] Z. N. Peterson, R. C. Burns, J. Herring, A. Stubblefield, and A. D. Rubin, "Secure deletion for a versioning file system.," in *File and Storage Technologies (FAST)*, vol. 5, pp. 4–11, 2005.

[15] A. S. Gajparia, C. J. Mitchell and C. Y. Yeun, "Supporting User Privacy in Location Based Services", in the Special issue on Mobile Multimedia Communications on IEICE Transactions on Communications, E88-B, 2837-2847, July 2005.

[16] A. S. Gajparia, C. Y. Yeun and C. Mitchell. "Using constraints to protect personal location information". In Proceedings of the 58th IEEE Semi-annual VTC 2003-Fall, Orlando, Florida, USA, 6-9 October 2003, Vol. 3, pp. 2112-2116.

[17] E. Al Alkeem, C. Y. Yeun, J. S. Baek, "Secure NFC Authentication Protocol Based on LTE Network", Lecture Notes in Electrical Engineering, Springer, Vol. 280, pp. 363-371, 2014.