Low Delay and Secure M2M Communication Mechanism for eHealthcare

Kashif Saleem, Abdelouahid Derhab
Center of Excellence in Information Assurance (CoEIA)
King Saud University (KSU)
Riyadh, Kingdom of Saudi Arabia (KSA)
{ksaleem, abderhab}@ksu.edu.sa

Jalal Al-Muhtadi
College of Computer and Information Sciences (CCIS),
King Saud University (KSU)
Riyadh, Kingdom of Saudi Arabia (KSA)
jalal@ccis.edu.sa

***Abstract*— Currently, the eHealthcare information management is the most critical and hot research topic. Especially with the involvement of new and promising telecommunication technologies like Machine to Machine (M2M) Communication. In M2M communication the devices interact and exchange information with each other in an autonomous manner to accomplish the required tasks. Mostly machine communicate to another machine wirelessly. The wireless communication opens the medium for enormous vulnerabilities and make it very easy for hackers to access the confidential information and can perform malicious activities. In this paper, we propose a Machine to Machine (M2M) Low Delay and Secure (LDS) communication system for e-healthcare community based on random distributive key management scheme and modified Kerberos realm to ensure data security. The system is capable to perform the tasks in an autonomous and intelligent manner that minimizes the workload of medical staffs, and improves the quality of patient care as well as the system performance. We show how the different actors in the e-healthcare community can interact with each other in a secure manner. The system handles dynamic assignments of doctors to specific patients. The proposed architecture further provides security against false attack, false triggering and temper attack. Finally, the simulation type implementation is performed on Visual Basic .net 2013 that shows the feasibility of the proposed Low Delay and Secure (LDS) algorithm.**

***Keywords*—Authentication, Decryption, eHealth, Encryption, Machine to Machine Communication, Malicious, Multihop, Random Key, Routing, Secure.**

I. INTRODUCTION

Providing a high quality patient care has always been a concern for healthcare community. There are many factors, which contribute to the high cost and low-quality of support offered to patients. Nursing facilities that assist patients through caregiver intervention and monitoring of the patient's health is costly. In addition, it represents a burden on caregiver who are unable to ensure continuous monitoring of the patient, which incurs low quality of care offered to the patients.

The appearance of e-healthcare systems has contributed in improving the quality of patient care and reducing the healthcare costs. By e-healthcare system, we mean a set of electronic tools: software and hardware designed to manage data in the healthcare system. The main components of the e-healthcare system include telemedicine, electronic health records, communication protocol among the components of the system.

Advances in the fields of sensor technologies, wireless networking technologies such as 3G, Wi-Fi, WiMax, Mesh networking, and personal area technologies like radio frequency identification (RFID) and Bluetooth have enabled the creation of a smart e-healthcare system, in which the medical staff can efficiently manage the health of the patients. Connecting tiny, low-power, and wearable smart medical sensor devices (e.g., pulse oximeters [1], electrocardiographs [2], and accelerometers [3]) to a human body has advanced the healthcare systems and allowed the appearance of potential applications such as: home monitoring for chronic and elderly patients [4], real-time continuous patient monitoring in hospitals [5], automated vital sign analysis to reduce the incidents due to human error [6], and emergency situations [7]. In these applications, the data collected by biosensors are transmitted to a server located at the hospital. The doctor can access the patient's records and monitor in real-time its health-conditions. In case of emergency, the doctor is notified by the system, as shown in Fig. 1.

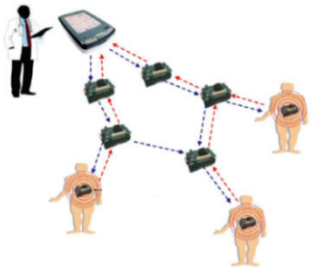

Figure 1. Architecture of e-healthcare system [8]

The above e-healthcare systems can significantly benefit both the medical staff and the patients. Firstly, it can ensure continuous and real-time monitoring of patient's conditions and solve the problem of inability to constantly monitor a patient's health. Secondly, the patients can minimize the cost of hospitalization while being monitored at their homes as effectively as in hospitals. Thirdly, remote and real-time monitoring help identifying the emergency conditions for patients in an easy and fast manner. Fourthly, it is possible to resolve the problem of unavailability of beds in hospitals by remotely monitoring some patients at their home instead.

All the above benefits offered by the e-healthcare system focus on the efficiency aspect, which is reducing the work overload on the medical staff and getting early responses in case of emergency. As in the scenario of smart ehealth care where remotely doctor is monitoring or providing treatment to his patient in hospital or in remote locations that can be patient's home, office or even while traveling. Overall realtime communication cannot tolerate any kind of delay or loss. The infrastructure should be reliable to provide guarantee services even the centralized management is available or not. Specially, when the time is very critical and rapid information is required [9]. Like in emergency conditions and disaster situation where top priority and error free services such as, rescue, transfer, treatment, stability, etc. are required, while providing the best security based on information availability of every individual [10].

In smart eHealthcare the Machine to Machine (M2M) communication is a new and emerging paradigm [11] that provides promising solutions. In M2M, the devices communicate and share information with each other autonomously as shown in Fig. 2 without or with limited human intervention [12].

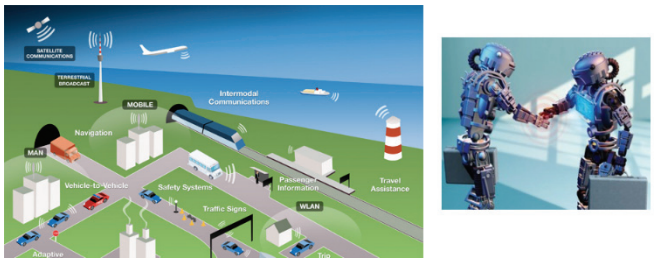

Figure 2. Future with M2M Communication [12]

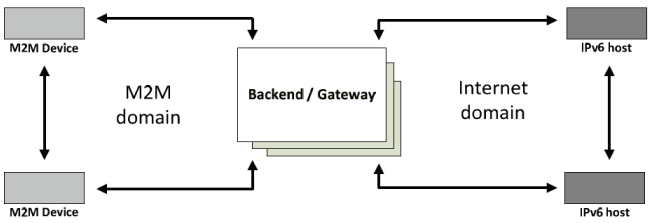

Figure 3. Machine to Machine (M2M) direct and Internet-integrated Communication [13]

M2M communication is used in a wide range of applications such as: smart home, smart e-health, smart grid, smart harvesting, etc [12]. In the literature, M2M communication has been proposed in many e-healthcare systems [14, 15]. The main challenge and aspect is security that needs to be addressed extensively before M2M communication is standardized and fully engaged in practical life [13]. Security in distributive and direct M2M communication as shown in Fig. 3, without centralized management is extremely critical [10, 16].

Little work is focusing on the security aspects of the M2M communication, and how to integrate security in M2M environments [13]. Due to the characteristics of the M2M communication such as heterogeneity, security issues must be addressed differently, and hence new security challenges are raised [17]. M2M systems need the integration of many technologies like: smart meters, sensing devices, mobile devices, RFID, Wi-Fi network, Low-Power Personal Area Networks, cellular network. This heterogeneity of communication technologies imposes on M2M applications to adopt new security design solutions to ensure privacy and data confidentiality [10].

As the M2M applications include low-size and self-powered energy constrained devices, the security solution needs to take into consideration the size of the cryptographic keys, the complexity of the cryptographic algorithm and the key management algorithms employed for the authentication, in order to not consume much energy [13]. In addition, the M2M applications should handle the security threats [18] and other attacks that can negatively affect correct functionalities [10].

- ✓ False network attack: When an M2M device is in detached state, an attacker can take the M2M device's identity (impersonation) communicate with the other components of the network and can receive some confidential information.
- ✓ False network triggering: As some M2M devices (eg. sensor mote) operate on low-power battery, they switch off their radio to save energy. An attacker continuously awaken the sleeping devices by sending them false network triggering in order to waste their energy consumption.
- ✓ Tamper attack: The trigger indication might contain the IP of the application server that the M2M device has to contact. If the IP address is tempered by an attacker, the M2M device may establish a connection to the wrong server, and hence it will be unable to communicate with the correct server and it will also waste its energy consumption.

The current standards [19] can handle or provide reliable communication in the specific mediums for what they built up for. These standardized protocols and security mechanisms can be used in M2M communication scenario, but after revision according to the application requirements, analysis and evaluation from all aspects [10]. Therefore, novel mechanisms are required to ensure the security of critical and confidential information over Machine to Machine (M2M) Communication.

In this paper, we propose a M2M Low Delay and Secure (LDS) communication system that is based on random key management authentication to ensure data privacy in M2M communication. The main contributions are

Firstly, we define the different interactions in M2M e-healthcare system, which can interact with each other in a secure manner. The security is ensured by involving intelligent authentication based on random distributive key management scheme, electronic certificate distribution, and modified Kerberos realm, while handling dynamic assignment of doctors to specific patient.

Secondly, the M2M system is designed to maximize the automated tasks, which reduces the workload of medical staffs, and further reduces the associated stress.

Thirdly, the Low Delay and Secure (LDS) Framework is implemented in Visual Basic .net 2013 to demonstrate the feasibility of the complete system.

Next section elaborates the most related and recent literature review. Section 3 describes the methodology of our proposed framework. Section 4 shows the implementation output. The conclusion and future work are discussed in section 5.

II. Related Work

M2M communication paradigm is one of the emerging research topics, and it fast adopted by many killer-application fields such as: Industrial monitoring and control, home automation, and health-care. Although, many M2M components related to networking decision, and choice of identity have been standardized, little work has done with respect to security. Also the research literature, which tackles M2M security, is very recent and less compared to other networks.

Nguyen and Huh [20] have proposed an authentication scheme to ensure the privacy property in a health-care application, which considers the mobility of doctors and patients in the hospital. The proposed scheme takes into consideration only the hospital space and does not discuss the possibility of extension to remote patients. Also, the authentication scheme is based on a probabilistic key management scheme, which can reduce the number of secured connections that can be established among the nodes composing the network.

Sun et al. [21] have proposed an M2M application that connects a mobile user with its home network. In order to ensure secure communication, password-based authentication and key establishment protocols are used between the nodes of the network. However, the proposed security scheme establishes secure connections with known communicating parties and cannot extend to more complex scenarios with dynamic associations between the users and the M2M devices.

The authors in [22], present a RelIable and SEcure Scheme (RISE) for M2M communication. To protect data confidentiality and integrity, the authors have developed a hash based function. The authors claim that the function under the proposed scheme defend M2M communication only against Target Distinguishing Attack. Furthermore, the given security architecture involves four algorithms, ChooseMedian, ChooseMost, ChooseNearest, and Trust-based Enhancement to provide data and device reliability. With data reliability the reports or data that are authenticated but discovered fake while checking at actuator based on four policies. Attainability of report is enhanced by implementing m repeat-sending and n multiple-reporting. The authors handle the behavior indistinguishability by hiding lasting time and the intervals while transmitting. The theoretical based formal analysis has been performed to show that the scheme is complete and sound. However, the author have not studied the performance evaluation and feasibility.

A. Research Gap

Security of M2M communication is an emerging and recent research topic. In this paper, we tackle some original security issues such as:

- ✓ How to design a low-delay architecture for the authentication scheme in the M2M networks.
- ✓ How to design an authentication scheme between two unknown communicating nodes in the M2M network.
- ✓ How to make the authentication scheme in the health-care scenario, which supports dynamic associations between the doctors and the patients.

III. Methodology

Under this section, the aspects of eHealthcare system is focused, initial design concept of the proposed security mechanism, security architecture, and its validation through implementation.

A. eHealthcare System Design

The principal members of the e-healthcare community, which participate in the proposed M2M communication system are shown in Fig. 4. In case of a patient or a group of patients there is a primary doctor and alternative doctors for each patient, who can remotely handle his/her case and intervene in case of emergency; Patient's family; Doctors; Nurses; Medical students; System administrator whose role is to assign doctors and medical students to patients, the assignment can be changed over time; Ambulance driver; and Pharmacist.

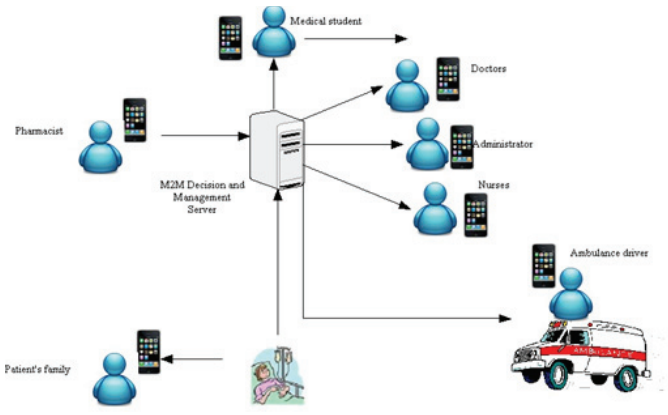

Figure 4. Human-Oriented Design of eHealthcare System

The members communicate among them using smartphones. Each smartphone includes a web-application that allows performing the e-healthcare system functionalities.

The system also includes M2M decision and management server: This server collects the data received from biosensors worn by the patients. We have utilized secure routing protocol [23] to securely transfer confidential information from biosensors to the base station that collects data. The server also helps in allowing the authorized medical staff to access the patient's data directly on patient side.

We define three scenarios of interactions among the members of the e-healthcare community:

1. Continuous data collection and data access: The biosensors continuously feed the M2M decision and management server with the patient's status and information. Each doctor, which is authorized to access these information (the current and the previous ones), can check the progress of the patient, send advices to the patients as well as authenticated prescriptions. The medical students can also access the patient's data to do research and survey studies.

2. Emergency detection: The emergency alarm is raised by the M2M decision and management server after analyzing the data received from the patient. For example if some data exceed a normal threshold, it is an indication of abnormal activities. Some statistical-based and data mining approaches can be used to take the appropriate decision such as: Markov chains [24], Dynamic Bayesian Network (DBN) [25], [26], [27], Hidden Markov Model (HMM) [27], and Conditional Random Fields (CRF) [28]. After detecting an abnormal activity that requires urgent intervention, the M2M server informs the primary doctor, the alternative doctors, as well as the patient's family member that is registered at the M2M communication system about the critical case of the patient.

   The system waits for any doctor which received the message to check the current patient's data and confirm whether the situation requires urgent medical intervention or not. After a short time period, if the M2M server does not receive any confirmation due to doctors' unavailability, it automatically decides to send message to the web-application of an ambulance driver at the hospital.

   If there is no response or all the drivers are busy, the server, using Google Map, looks for the closest hospital to the patient and contacts the M2M server of this hospital to send an ambulance to the patient. After that, the M2M server informs some doctors and nurses, which are available at the hospital, to prepare for treatment in advance of the arrival of the patient.

3. Prescription Management: The doctor, which accesses the data of its patient, can judge that there is a need to issue a prescription for this patient. The doctor signs the prescription using its electronic certificate. The M2M server sends the prescription to the patient's smartphone. When the patient goes to the pharmacy, the pharmacist, by checking the electronic signature, can verify the authenticity of the prescription

B. *Design concept of Low Delay and Secure (LDS) Framework*

The initial concept of Low Delay and Secure (LDS) Framework for M2M communication in health care scenario [9] is shown in Fig. 5. Every connection in between machines is based on public and private key mechanism [21, 29] as shown in Fig. 5, to validate and to transfer data securely. The key management system and information is mainly taken care by the centralized servers, and modified Kerberos realm [29, 30] as shown in Fig. 6, will be employed according to application. If the main server is not available and/or machines are very near to each other than certificate based authentication will be performed directly in between the two machines to completely secure M2M communication [9].

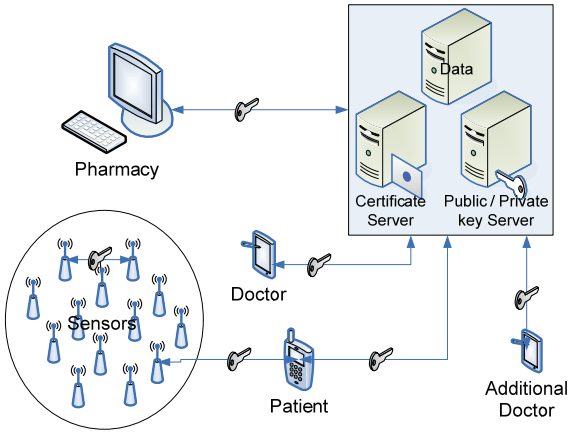

Figure 5. Initial Concept of LDS

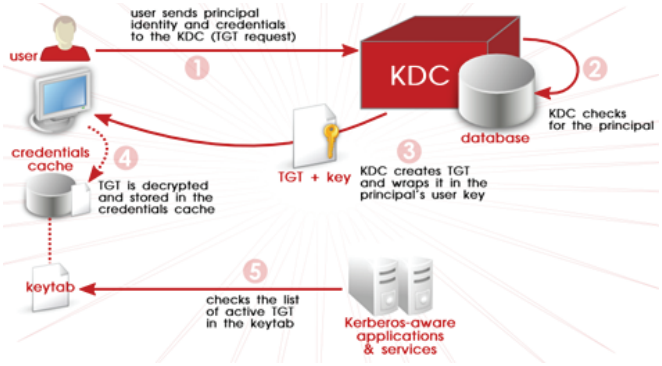

Figure 6. Kerberos Realm [29]

The direct communication will reduce the delay and is online. For instance, if the authorized doctor is with the patient, his mobile application will directly communicate with the patient handheld device to acquire the current readings. As soon as the server got available the doctors mobile will be updated will the other details of the current patient.

Devices can be equipped on the body of the patient or/and can be deployed around in the overall structure to monitor the patient and patient's environment. The distributive mechanism will be managed with the help of the modified concept based on Kerberos Realm [29] according to application requirements as shown in Fig. 6.

C. LDS Design Approach

The design of the proposed LDS Security mechanism is shown in Fig. 7. The process begins when two devices or machines, which need to exchange the information. First the algorithm checks the server availability, if it is available it will check for the updated certificates and security information from server. Otherwise, the current node will authenticate based on the local certificate. After the authentication process completed the exchange key process will be invoked. If the keys are exchanged successfully the encrypted information will start transferring, else again the authentication will be re-performed.

The key based certificate and encryption mechanism can ensure the authentication of users and confidentiality of data. Therefore, the proposed LDS can prevent communication from false attack, false triggering and temper attack.

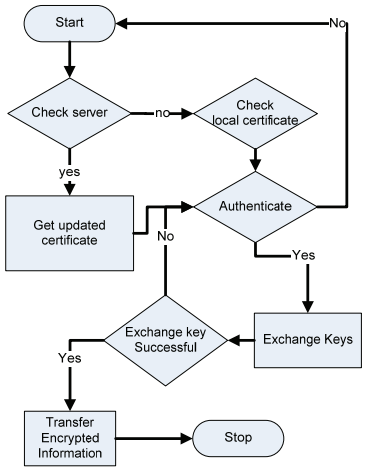

Figure 7. State Machine Diagram of Packet Encryption and Decryption

IV. IMPLEMENTATION

We have implemented the Fig. 5 scenario under Visual Basic .net 2013 and the screenshot is shown in Fig. 8. The simulation type based implementation is performed to analyze the output of applied algorithms. Under analysis, we study whether the LDS based on Kerberos is working and giving output according to required expectations or not. In the program, we enable a database with some entities as Patient ID, ECG and Blood pressure and other database as shown in Fig. 9 with Kerberos Key Distribution Center (KDC). On frontend the frame based mobile display is authenticated by the database.

The certificate is given to the frontend mobile display and stored in the variable. Onward, the mobile display frame is authenticated by the communicator based on offline certificate in variable and can acquire the data directly from the patient embedded devices. The main database updates all the certificates when the KDC database is updated. The remote patient's data (randomly generated numbers) is periodically (after every 5 minutes) coming in and recorded the main database as shown in Fig. 9. The records that are coming to the database are encrypted and is decrypted based on the key assigned to the user, otherwise the record is discarded. The doctors at remote locations can acquire the data of remote patient directly, if the mobile application is pre-authenticated and offline certificate is stored in it. Otherwise, the connection to main server is essential to complete the authorization and authentication processes.

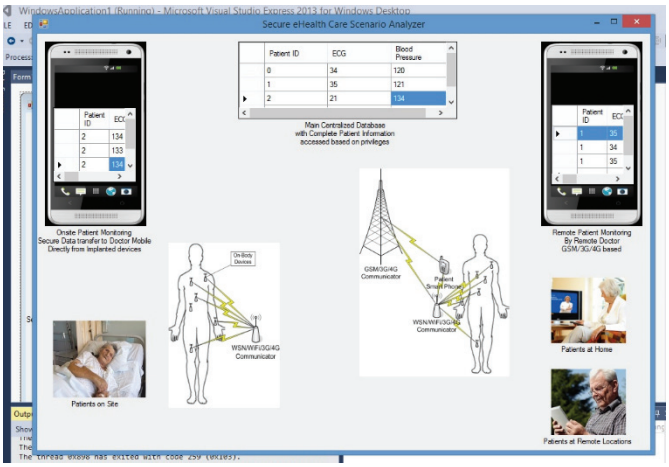

Figure 8. Mechanism Implementation

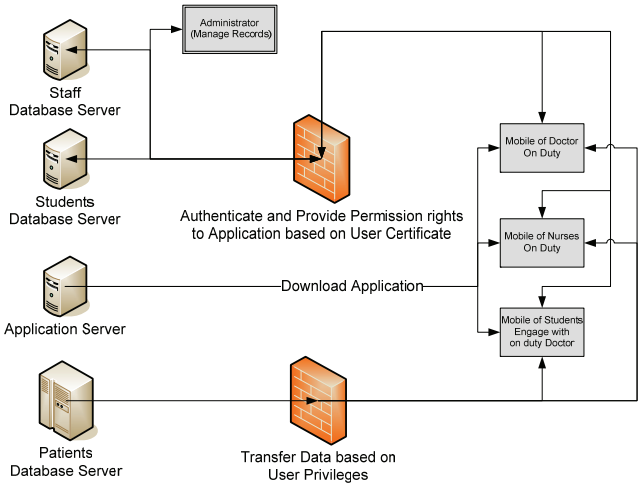

Figure 9. Backend Functioning of Implementation

V. CONCLUSION AND FUTURE WORK

In this paper, we have propose a Machine to Machine (M2M) communication system that aims at performing most of the tasks automatically in an autonomous and intelligent manner and without human intervention, which minimizes the workload of medical staffs. We have shown that the interactions among the e-healthcare community member in a secure manner. To ensure data privacy, the mechanism involves intelligent authentication based on random distributive key management scheme and modified Kerberos realm while handling dynamic assignment of doctors to specific patient. The proposed architecture provides security against false attack, false triggering and temper attack. The given scenario is implemented in Visual Basic .net 2013 that shows the feasibility of the proposed Low Delay and Secure (LDS) Framework.

In future, we will evaluate the proposed system experimentally by implementing the scenario in real world.

ACKNOWLEDGMENT

This work is supported by the Research Center of College of Computer and Information Sciences, King Saud University, Grant Number RC140224. The authors are grateful for this support.

REFERENCES

[1] N. M. Inc. (2014, 28 May). *Avant 4000 Wireless Wearable Pulse Oximeter. A1 207-408*. Available: http://www.medicalproductsdirect.com/puoxnoav40pu.html

[2] T. R. F. Fulford-Jones, W. Gu-Yeon, and M. Welsh, "A portable, low-power, wireless two-lead EKG system," in *Engineering in Medicine and Biology Society, 2004. IEMBS '04. 26th Annual International Conference of the IEEE*, 2004, pp. 2141-2144.

[3] M. J. Mathie, A. C. Coster, N. H. Lovell, and B. G. Celler, "Accelerometry: providing an integrated, practical method for long-term, ambulatory monitoring of human movement," *Physiol Meas,* vol. 25, pp. R1-20, Apr 2004.

[4] E. Dishman, "Inventing wellness systems for aging in place," *Computer,* vol. 37, pp. 34-41, 2004.

[5] K. Van Laerhoven, B. P. Lo, J. W. Ng, S. Thiemjarus, R. King, S. Kwan*, et al.*, "Medical healthcare monitoring with wearable and implantable sensors," in *Proc. of the 3rd International Workshop on Ubiquitous Computing for Healthcare Applications*, 2004.

[6] R. Ohmura, F. Naya, H. Noma, N. Kuwahara, T. Toriyama, and K. Kogure, "Practical Design of A Sensor Network for Understanding Nursing Activities," in *Local Computer Networks, Proceedings 2006 31st IEEE Conference on*, 2006, pp. 615-622.

[7] K. Lorincz, D. J. Malan, T. R. F. Fulford-Jones, A. Nawoj, A. Clavel, V. Shnayder*, et al.*, "Sensor Networks for Emergency Response: Challenges and Opportunities," *IEEE Pervasive Computing,* vol. 3, pp. 16-23, 2004.

[8] E. E. Egbogah and A. O. Fapojuwo, "A survey of system architecture requirements for health care-based wireless sensor networks," *Sensors (Basel),* vol. 11, pp. 4875-98, 2011.

[9] F. Zhong and T. Siok, "M2M communications for e-health: Standards, enabling technologies, and research challenges," in *Medical Information and Communication Technology (ISMICT), 2012 6th International Symposium on*, 2012, pp. 1-4.

[10] C. Lai, L. Hui, Z. Yueyu, and C. Jin, "Security Issues on Machine to Machine Communications," *KSII Transactions on Internet & Information Systems,* vol. 6, pp. 498-514, 2012.

[11] M. Chen, J. Wan, and F. Li, "Machine-to-Machine Communications: Architectures, Standards and Applications," *KSII Transactions on Internet & Information Systems,* vol. 6, pp. 480-497, 2012.

[12] Z. Yan, Y. Rong, X. Shengli, Y. Wenqing, X. Yang, and M. Guizani, "Home M2M networks: Architectures, standards, and QoS improvement," *Communications Magazine, IEEE,* vol. 49, pp. 44-52, 2011.

[13] J. Granjal, E. Monteiro, and J. Silva, "Security Issues and Approaches on Wireless M2M Systems," in *Wireless Networks and Security*, S. Khan and A.-S. Khan Pathan, Eds., ed: Springer Berlin Heidelberg, 2013, pp. 133-164.

[14] C. Min, W. Jiafu, S. Gonzalez, L. Xiaofei, and V. C. M. Leung, "A Survey of Recent Developments in Home M2M Networks," *Communications Surveys & Tutorials, IEEE,* vol. 16, pp. 98-114, 2014.

[15] S. J. Jung, R. Myllyla, and W. Y. Chung, "Wireless Machine-to-Machine Healthcare Solution Using Android Mobile Devices in Global Networks," *Sensors Journal, IEEE,* vol. 13, pp. 1419-1424, 2013.

[16] D. Chen and G. Chang, "A Survey on Security Issues of M2M Communications in Cyber-Physical Systems," *KSII Transactions on Internet & Information Systems,* vol. 6, pp. 24-45, 2012.

[17] C. Inhyok, Y. Shah, A. U. Schmidt, A. Leicher, and M. V. Meyerstein, "Trust in M2M communication," *Vehicular Technology Magazine, IEEE,* vol. 4, pp. 69-75, 2009.

[18] J. Partala, Kera, x, N. nen, Sa, x*, et al.*, "Security threats against the transmission chain of a medical health monitoring system," in *e-Health Networking, Applications & Services (Healthcom), 2013 IEEE 15th International Conference on*, 2013, pp. 243-248.

[19] A. Hommersom, P. J. F. Lucas, M. Velikova, G. Dal, J. Bastos, J. Rodriguez*, et al.*, "MoSHCA - my mobile and smart health care assistant," in *e-Health Networking, Applications & Services (Healthcom), 2013 IEEE 15th International Conference on*, 2013, pp. 188-192.

[20] N. Mui Van, A. Al-Saffar, and H. Eui-Nam, "A dynamic ID-based authentication scheme," in *Networked Computing and Advanced Information Management (NCM), 2010 Sixth International Conference on*, 2010, pp. 248-253.

[21] X. Sun, S. Men, C. Zhao, and Z. Zhou, "A security authentication scheme in machine-to-machine home network service," *Security and Communication Networks,* pp. n/a-n/a, 2012.

[22] W. Ren, L. Yu, L. Ma, and Y. Ren, "RISE: A RelIable and SEcure scheme for wireless Machine to Machine communications," *Tsinghua Science and Technology,* vol. 18, pp. 100-117, 2013.

[23] K. Saleem, N. Fisal, and J. Al-Muhtadi, "Empirical Studies of Bio-inspired Self-Organized Secure AutonomousRouting Protocol," *Sensors Journal, IEEE,* vol. PP, pp. 1-8, 2014.

[24] A. Mihailidis, J. Boger, M. Canido, and J. Hoey, "The use of an intelligent prompting system for people with dementia," *interactions,* vol. 14, pp. 34-37, 2007.

[25] T. van Kasteren and B. Krose, "Bayesian activity recognition in residence for elders," in *Intelligent Environments, 2007. IE 07. 3rd IET International Conference on*, 2007, pp. 209-212.

[26] D. H. Wilson and C. Atkeson, "Simultaneous Tracking and Activity Recognition (STAR) Using Many Anonymous, Binary Sensors," in *Pervasive Computing*. vol. 3468, H.-W. Gellersen, R. Want, and A. Schmidt, Eds., ed: Springer Berlin Heidelberg, 2005, pp. 62-79.

[27] A. Subramanya, A. Raj, J. A. Bilmes, and D. Fox, "Recognizing Activities and Spatial Context Using Wearable Sensors," presented at the UAI, 2006.

[28] M. Philipose, K. P. Fishkin, M. Perkowitz, D. J. Patterson, D. Fox, H. Kautz*, et al.*, "Inferring activities from interactions with objects," *Pervasive Computing, IEEE,* vol. 3, pp. 50-57, 2004.

[29] W. Stallings, *Cryptography and Network Security (4th Edition)*: Prentice Hall, 2005.

[30] D. Inshil, C. Kijoon, L. Jiyoung, and C. Min Young, "An Improved Security Approach Based on Kerberos for M2M Open IPTV System," in *Network-Based Information Systems (NBiS), 2012 15th International Conference on*, 2012, pp. 754-759.