Human-oriented design of secure Machine-to-Machine communication system for e-Healthcare society

Kashif Saleem, Abdelouahid Derhab, Jalal Al-Muhtadi, Basit Shahzad

Abstract

In this paper, we propose a Machine to Machine (M2M) Low Cost and Secure (LCS) communication system for e-Healthcare society. The system is designed to take into consideration the psychological issues related to all actors in the e-Healthcare society such as: stress due to high workload, anxiety, and loneliness. The system is capable of performing most of the tasks in an autonomous and intelligent manner, which minimizes the workload of medical staffs, and consequently minimizes the associated psychological stress and improves the quality of patient care as well as the system performance. We show how the different actors in the e-Healthcare society can interact with each other in a secure manner. To ensure data privacy, the mechanism involves intelligent authentication based on random distributive key management, electronic certificate distribution, and modified realm Kerberos. The system handles dynamic assignments of doctors to specific patients. It also addresses the need for patients to share their health information with strangers while dealing with the privacy preservation issue. Finally, the simulation type implementation is performed on Visual Basic .net 2013 that shows the success of the proposed Low Cost and Secure (LCS) algorithm.

1. 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 are costly. In addition, it represents a burden on caregiver who is 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 such as 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 (Inc., 2014), electrocardiographs (Fulford-Jones, Gu-Yeon, & Welsh, 2004), and accelerometers (Mathie, Coster, Lovell, & Celler, 2004)) 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 (Dishman, 2004), real-time continuous patient monitoring in hospitals (Van Laerhoven et al., 2004), automated vital sign analysis to reduce the incidents due to human error (Ohmura et al., 2006), and emergency situations (Lorincz et al., 2004). 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 locally as well as remotely from these servers and thus can real-time monitor patient’s health-conditions. In case of emergency, the doctor is notified by the system, as shown in Fig. 1.

Machine to Machine (M2M) communication is a new and emerging paradigm under telecommunication (Chen, Wan, & Li, 2012). In M2M, the devices communicate and share information with each other autonomously without or with limited human intervention (Yan et al., 2011). M2M communication is used in a wide range of applications such as: smart home, smart e-Health,
smart grid, and smart harvesting (Booysen, Gilmore, Zeadally, & Van Rooyen, 2012; Yan et al., 2011). In the literature, M2M communication has been proposed in many e-Healthcare systems (Jung, Ahn, Hwang, & Kim, 2012; Jung, Myllyla, & Chung, 2013; Min, Jiafu, Gonzalez, Xiaofei, & Leung, 2014; Park, Jung, Shin, Kim, & Yoon, 2014).

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 helps 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. However, the psychological issues, which come along with the illness, are not considered when designing e-Healthcare system. Physical illness is stressful experience and often puts emotional pressure, and burden on all the members of the healthcare society including the medical staff, patients and their families. It is known that physical symptoms often have an underlying psychological component. All illnesses have a psychological impact because illness is a threat to self. Depression loneliness and anxiety are common in illness, especially in chronic or life-threatening illnesses. The patients also need social support and share their feelings and concerns about the illness usually to strangers without the need to reveal their identities. On the other hand, medical staff are experiencing high level of stress caused by the heavy workload.

In this paper, we propose a M2M Low Cost and Secure (LCS) communication system, which considers the psychological issues of medical staff and patients when designing the healthcare system. A part of this work as a preliminary report has been presented previously in (Saleem, Derhab, & Al-Muhtadi, 2014). The main contributions of this paper are the following: 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 realm Kerberos, 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 system also provides access to online support groups and addresses the need for patients to share their health information with strangers while dealing with the privacy preservation issue. The Low Cost and Secure (LCS) Framework is implemented in Visual Basic.net 2013 to analyze the effectiveness of the complete system.

The rest of the paper is organized as follows: Section 2 gives an overview of Machine to Machine (M2M) communication and presents related work on secure M2M communication systems. In Section 3, we describe the Human-centered design of our proposed M2M communication system for e-Healthcare society. Section 4 describes the security design of the proposed system. In Section 5, the prototype implementation is described. Finally, Section 6 concludes the paper and outlines perspectives for further works.

2. Machine to Machine (M2M) communication

Machine to Machine (M2M) communication is a new and emerging paradigm under telecommunication (Chen et al., 2012). M2M communication is used in a wide range of applications such as: smart home, smart e-Health, smart grid, and smart harvesting (Booysen et al., 2012; Yan et al., 2011). The general architecture of M2M communication is shown in Fig. 2, and is composed of the following components: M2M device, M2M domain, and Internet domain. M2M device can be computers, sensors, actuators, embedded and mobile devices that communicate and share information with each other autonomously without or with limited...
human intervention and via wired or wireless network (Yan et al., 2011). M2M domain provides connectivity between the M2M device and the gateway. The Internet domain ensures communication between the gateway and the M2M application at the host. The main advantage of M2M communication is that the devices interact with each other to collect and deliver the required real-time information. Every device in M2M domain almost communicates wirelessly and acts as the server to help overall network in performing the given task as shown in Fig. 2. The wireless un-attendant communication nature opens enormous challenges for M2M.

An e-Healthcare scenario as an example of M2M communication is shown in Fig. 3. In the case of remote patient monitoring, sensor devices that are worn by a patient form a body area network (BAN) to record health indicators, e.g., blood pressure, body temperature, heart rate (Saleem, Fisal, & Al-Muhtadi, 2014). The sensors forward the collected data to an M2M gateway that acts as an information aggregator. Then, the aggregator forwards the data to the M2M server via communication networks. The M2M server analyzes the collected data and sends warnings and appropriate medical records to the medical staffs. In emergency cases, an M2M device can directly provide the medical status of a patient and route to the hospital, allowing physicians to prepare for treatment in advance of the arrival of the patient. The real-time communication cannot tolerate any kind of delay or loss. The infrastructure should be reliable to provide guarantee services whether the centralized management is available or not. Specially, when the time is very critical rapid information is required (Zhong & Siok, 2012), like in emergency conditions and disaster situation where top priority and error-free services such as; rescue, transfer, treatment, and stability are required (Lai, Hui, Yueyu, & Jin, 2012).

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 (Mui Van, Al-Saffar, & Eui-Nam, 2010) 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, Men, Zhao, and Zhou (2012) 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.

Ren, Yu, Ma, and Ren (2013) 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 defends M2M communication only against Target Distinquishing 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 \textit{m} repeat-sending and \textit{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 has not studied the performance evaluation and feasibility.
The authors in (Inshil, Kijoon, Jiyoung, & Min Young, 2012), proposed a security approach for M2M communication in open IPTV system. The given approach provides secure user authentication with Kerberos based key distribution. The authors modify Condition Access System (CAS) to reduce the complexity and enhance the efficiency of authentication process. The process depends on stages that starts by contents information transfer and ticket request, then to access service provider ticket is granted by ticket server (TS), and in the end the Service user authentication and obtaining of service are granted. To perform analysis the authors set up a network with ten users around TS and Authentication Server (AS). The outcomes are compared with traditional user authentication mechanisms for IPTV in terms of processing time. The proposed approach has shown better performance, but the strength against malicious activities has not been tested.

3. Human-oriented design of e-Healthcare system

As stated above, the medical staff are experiencing stress caused by heavy workload. This psychological issue can be minimized by maximizing the tasks performed by the M2M communication system. On the other hand, the issues of depression loneliness, and anxiety are handled by providing emotional support through access to online support groups. Health-related Online Supported Groups have become an important source for information and support for patients (Chung, 2013), and these online groups are more advantageous of face-to-face ones. Liang, Barua, Lu, Lin, and Shen (2012) proposed HealthShare, a health social network, which allows patients to share their health information and preserve their privacy. In our M2M communication system, we propose two ways for patients to get online social support: one way is from a social network formed among the patients that are registered at the M2M communication system of the hospital. The second way is to provide information and links about other online groups, which can provide social and psychological support to the patients.

The principal members of the e-Healthcare society, which participate in the proposed M2M communication system are shown in Fig. 4 and are as follows:

- One or a group of patients: For each patient, there is a primary doctor and alternative doctors 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.
- Pharmacist.

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 two main components:
M2M decision and management server: This server collects the data received from biosensors worn by the patients. It also, allows the authorized medical staff to access the patient’s data.

Privacy-based social network under the control of the system administrator. In this network, the real identity of patients is not disclosed.

We define four scenarios of interactions among the members of the e-Healthcare society: (1) Continuous data collection and data access, (2) emergency detection, (3) prescription management, and (4) accessing privacy-based social network.

3.1. 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, who 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.

3.2. 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 (Mihailidis, Boger, Canido, & Hoey, 2007), Dynamic Bayesian Network (DBN) (Subramanya, Raj, Bilmes, & Fox, 2006; van Kasteren & Krose, 2007; Wilson & Atkeson, 2005), Hidden Markov Model (HMM) (Subramanya et al., 2006), and Conditional Random Fields (CRF) (Liyue, Xi, Sukthankar, & Sukthankar, 2010; Philipose et al., 2004).

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 who 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 GoogleMap, looks for the closest hospital for 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, who are available at the hospital, to prepare for treatment in advance of the arrival of the patient.

3.3. Prescription management

The doctor, who accesses the data of their patient, can judge that there is a need to issue a prescription for this patient. The doctor signs the prescription using their 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.

3.4. Accessing privacy-based social network

The administrator can register the patients on the social network of the M2M communication of the e-Healthcare system. The patients are registered under pseudonyms and their identities are not disclosed. The patients are also provided with a list of online groups that can give social and psychological supports.

4. Security design of the M2M communication e-Healthcare system

4.1. Security requirements of M2M communication

For most of the applications using M2M devices, security is one of the critical requirements (Chen & Chang, 2012). Little work is...
focusing on the security aspects of the M2M communication, and how to integrate security in M2M environments (Granjal, Monteiro, & Silva, 2013). Due to the characteristics of the M2M communication such as heterogeneity, security issues must be addressed differently, and hence new security challenges are raised (Inhyok, Shah, Schmidt, Leicher, & Meyerstein, 2009). M2M systems need the integration of many technologies such as: 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 (Lai et al., 2012). 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 optimize energy consumption (Granjal et al., 2013).

The current standards can handle or provide reliable communication in the specific mediums for what they built up for. These standardized protocols (Saleem, 2006; Saleem & Fisal, 2012; Saleem et al., 2009; Zubair, Fisal, Baguda, & Saleem, 2013) and security mechanisms (Saleem, Fisal, Hafizah, & Rashid, 2011; Saleem, Khalil, Fisal, Ahmed, & Orgun, 2013) can be used in M2M communication scenario, but after revision according to the application requirements, analysis and evaluation from all aspects (Lai et al., 2012). Therefore, novel mechanisms are required to ensure the security of critical and confidential information over Machine to Machine (M2M) communication.

Please cite this article in press as: Saleem, K., et al. Human-oriented design of secure Machine-to-Machine communication system for e-Healthcare society. Computers in Human Behavior (2014), http://dx.doi.org/10.1016/j.chb.2014.10.010
4.2. Research gap

Security of M2M communication is an emerging and recent research topic and there is a plenty of rooms for contributions. In this section, we are going to tackle some original security issues such as:

- How to design a low-cost 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.

4.3. Design concept of Low Cost and Secure (LCS) framework

The aspects that will be focused more are the initial design concept of the proposed security mechanism, security architecture, its performance evaluation and validation. The initial concept of Low Cost and Secure (LCS) Framework for M2M communication in health care scenario (Zhong & Siok, 2012) is shown in Fig. 5. Every connection between machines is based on public and private key mechanism (Stallings, 2005; Sun et al., 2012) as shown in Fig. 5, to validate and to transfer data securely.

The key management system and information are mainly taken care by the centralized servers, and modified Kerberos (Inshil et al., 2012; Stallings, 2005) 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 then certificate based authentication will be performed directly between the two machines to completely secure M2M communication (Zhong & Siok, 2012).

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 becomes available, the doctors mobile will be updated with 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’s environment. The distributive mechanism will be managed with the help of the modified concept based on Kerberos Realm (Stallings, 2005) according to application requirements as shown in Fig. 7.

---

**Fig. 8.** State machine diagram of packet encryption and decryption.

**Fig. 9.** Backend functioning.
4.4. LCS design approach

The design of the proposed LCS Security mechanism is shown in Fig. 8. The process begins when two devices or machines 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.

5. Prototype implementation

We have implemented Fig. 5 scenario under Visual Basic .net 2013 and the screenshot is shown in Fig. 10. The simulation type based implementation is performed to analyze the output of applied algorithms. Under analysis, we study whether the LCS based on Kerberos is working and giving output according to required expectations or not. In the programme, we enable a database with some entities as Patient ID, ECG and blood pressure and other databases 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) are periodically (after every 5 min) coming in based on (Saleem, Fisal, Hafizah, Kamilah, & Rashid, 2009; Saleem et al., 2014) and recorded in the main database as shown in Fig. 9. The records that are coming to the database are encrypted and 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. At the end we perform the risk assessment based on the phases given in (Mathkour, Shahzad, & Al-Wakeel, 2011; Shahzad & Al-Mudimigh, 2010; Basit Shahzad, Iqbal, ul Haq, & Raza, 2006; Basit Shahzad & Safvi, 2010) to assure the quality of the software.

6. Conclusion and future work

In this paper, we have proposed a Machine to Machine (M2M) communication system that takes into consideration the psychological issues related to the actors of the e-Healthcare society such as: stress due to high workload, anxiety, loneliness. The system 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 as well as the associated stress. This leads to an improvement of the patient care quality and the system performance in terms of execution durations of the tasks. We have shown the members composing the e-Healthcare society as well as the interactions among the members in a secure manner. To ensure data privacy, the mechanism involves intelligent authentication based on random distributive key management scheme and
modified realm Kerberos while handling dynamic assignment of doctors to specific patient. The system also addresses the need for patients to share their health information with strangers while dealing with the privacy preservation issue. This is achieved by registering the patients to the privacy-based social support group managed by the system administrator and providing them with a list of online groups that can provide such supports. The given scenario is implemented in Visual Basic.net 2013 that shows the effectiveness of the proposed Low Cost and Secure (LCS) Framework. Due to the fact that M2M communication makes the interconnection between devices more complex, new security threats have been emerged. As a future work, we are going to study the effect of these threats on the decision process in the healthcare society and analyze the security resilience of LCS. In addition, we plan to study how LCS can be integrated in other application fields such as: industrial automation, smart home, and smart grid.

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


Article in Press


Please cite this article in press as: Saleem, K., Human-oriented design of secure Machine-to-Machine communication system for e-Healthcare society. Computers in Human Behavior (2014), http://dx.doi.org/10.1016/j.chb.2014.10.010

9