A SECURE DATA SHARING SCHEME IN PUBLIC CLOUD FOR ECG SIGNAL MONITORING APPLICATION

Malathi.S[1], Dr. L. Malathi[2]

[1]P.G Scholar, Dept of Computer Science Engineering,Vivekanandha College of Engineering for Women, Tamilnadu, India
[2]Head of Department, Dept of Computer Science Engineering,Vivekanandha College of Engineering for Women, Tamilnadu, India

---***---

Abstract - *To achieve secure communications in wireless sensor networks (WSNs), sensor nodes (SNs) must establish secret shared keys with neighboring nodes. Moreover, those keys must be updated by defeating the insider threats of corrupted nodes. to propose a location-based key management scheme for WSNs, with special considerations of insider threats. After reviewing existing location-based key management schemes and studying their advantages and disadvantages, to selected location dependent key management (LDK) as a suitable scheme for our study. To solve a communication interference problem in LDK and similar methods, we have devised a new key revision process that incorporates grid-based location information. And also propose a key establishment process using grid information. Furthermore, to construct key update and revocation processes to effectively resist inside attackers. For analysis, to conducted a rigorous simulation and confirmed that our method can increase connectivity while decreasing the compromise ratio when the minimum number of common keys required for key establishment is high. When there was a corrupted node leveraging insider threats, it was also possible to effectively rekey every SN except for the corrupted node using our method.*

1. INTRODUCTION

The Internet has changed the way of life for most people in the last decade. Information is exchanged via email or instant messaging and it evolved from a tool for experts to a connector of people all over the world. And it is still evolving. One of these evolutions is the integration of more and more devices into the Internet. Today most of the new TV sets are Internet capable and the Internet of Things tries to incorporate most electronic devices in the near future. One of the enabling technologies to access and use even the smallest device are Wireless Sensor Networks (WSNs). With advances in miniaturization of electronic components and enhanced performance over the last decade, smart electronic devices are penetrating more and more areas of daily life. Application areas for WSNs range from agriculture or logistics to health care and emergency response scenarios. These applications can be split into several (sub-)tasks. Depending on the scenario a sensor network can span from some rooms to an area of several square miles in size and so the number of sensor nodes can vary from a fistful of nodes to hundreds or thousands. Sensor nodes are composed from a set of building blocks: processing, communication capabilities, sensing/actuating and power supply. The large

Quantities of nodes participating in sensor networks has pushed prices down. These nodes consist of a slow CPU combined with a limited amount of memory. This allows pre-processing or decision taking on the local node before reporting data via a communication link or triggering some kind of actuation. The transceiver is most of the time a low-bandwidth radio link, but also other techniques like infrared are possible. Sensing/actuation depends on the actual application, many sensors or actuators are possible here. The power supply is usually a battery pack. The low cost requirements result in highly constrained resources on a sensor node. This requires suitable and efficient algorithms, optimized for the limited CPU and memory space. Especially the limited energy resources make it tremendously important to save resources to achieve a long lifetime. Transmitting messages requires a significant amount of energy and, therefore, as few messages as possible are sent. Messages should be kept as short as possible. The range of the transceivers used is typically limited and messages are sent in a multi-hop fashion, i.e. a message is received by a node and then forwarded to its destination, hop by hop. Today's WSNs are planned and developed to satisfy only one application, and they are usually controlled by a single user.

2. HEADING

2.1 Global burden of Cardiovascular Disease

Cardiovascular disease (CVD), a global burden or 'global epidemic' (WHO, 2004) of disease which cause the premature mortality of 17 million of people each year. The statistic even more surprisingly in American as reported by American Heart Association, approximate 2300 Americans die from CVD each day and average of 38 seconds for each occurs (Lloyd-Jones et al., 2010). Cardiovascular disease causing the burden of economic in country as large amount of funds allocated in disease diagnostic and healthcare. Figure 2.1 shows the full-income losses due to heart disease, stroke and diabetes in 2005 compared with 2015 estimate. China encounters approximate 450 billion losses as compared to others countries(Organization, 2005). In Malaysia, the statistic of cardiovascular disease cannot be neglect. In a Burden of Disease study in 2004, cardiovascular disease contribute two third among the burden of disease in Malaysia (Malaysia Health, 2008). According to Health Fact 2013, the disease of circulatory system is the top disease which encountered around 24.69% of death in Ministry of Health Hospital (MOH) Malaysia.

These statistic shows that the cardiovascular disease is the major life threatened disease compared to other diseases. Therefore, it is reasonable to classify it as a global burden of disease as it causes the mortality and disability of millions of generations. Also, large amount of fund allocated for disease diagnostic and treatment which is a burden of economic in the development country. Financial allocation for MOH in year 2013 was estimate by RM 19.28 billion for operating and development (Health Facts, 2013).

2.1.1 Stroke caused by Arrhythmias

According WHO report, 15 millions of people suffer from stroke disease each year. Among this, 5 million are death and 5 million people permanently disable. Among this, there is one people suffer from stroke due to atrial fibrillation in every four minutes (Heart & Stroke Foundation, 2010). This clearly shows the impact of heart disease not only causes death, but also the possibility of causing permanently disable.

The key to early and regular screening of the heart is not only to prevent heart attack but also to prevent stroke. Stroke can cause severe weakness, requires prolonged rehabilitation, and is extremely expensive to any healthcare system.

2.2 Strategies in Reduce Disease

Malaysian government had treated this issue as an urgent issue to be solved immediately. Ischaemic heart disease is one of the top diseases that emphases in the Nine Malaysia Plan with the goal of disease prevent and reduce (NSPNCD, 2010). This statement is further support in the Country Health Plan (10th Malaysia Plan, 2011-2015), government producing the Healthy Public Policy which is the Wellness Policy. This policy mainly focus on changing the illness to wellness by promote the early self-assessment in the community as the cardiovascular disease is one of the burden diseases in Malaysia.

1Malaysia clinics is one of the Healthcare facilities promote by government Malaysia to encourage more and more public to assess their health with the current 178 units of clinics available in Malaysia(Health Fact, 2013). Residences encourage having regular body check-up as a precaution and early detection of any disease.

As defined by World Health Organization (WHO), disease such as diabetes, heart disease and hypertension can be included in the category of non-communicable disease (NCD). According to Datuk Seri Dr Hasan Abdul Rahman, the Director-general of Health, "Malaysians do not realise that NCD can be controlled if detectedearly." (New Strait Times, May 2012). Early of disease detection is very important to increase the change of recover and illness control.

2.3 Tools in Disease Diagnosis

2.3.1 Introduction to ECG Machine

One of the diagnostic tools use in heart diseases detection is Electrocardiography (ECG) which allows great insight in regularity of heart functioning by using a series of analysis algorithms. Electrocardiography is a device used in evolution and recording of the heart's electrical activity using a graphical representation, also called Electrocardiogram (ECG) (Shade and Wesley, 2006). By comparing the vital pattern with the available database, the types of heart disease can be detected if the electricity generated versus time is deflected from the normal range which usually called Dysrhythmias. ECG plays an important role in assessing the evaluation and response to treatment for heart pathologies.

The ECG was introduced by William Einthoven (1860-1927) in 1893 and the first ECG monitor was built in 1901. Conventional ECG monitor limits the mobility and measurement time of patients which is impractical for long terms used (Kai et al., 2011). Also, the results might show normal during the diagnostic while it's actually critically diseased (Davey, 2004). This can be evidence by around 5-10% of coronary heart disease's patient show a normal ECG recording and without any symptoms (Luna, 2007). This lead to misinterpretation of cardiologist and causing around half of the cardiac death occurs outside the hospital. In 1949, Holter innovate the ambulatory ECG monitor for the purpose of pre-assessing patient's condition to prevent delay of rescue time (David et al., 2006). Despite of limitation of ECG monitoring at hospital level, revolution of ECG comes with introducing Holter ECG which improved in terms of its portability, size and allow patient to do the self-assessment outside the hospital. Although the invention of Holter ECG increased the mobility of patient, limitations still exist in terms of its convenience and eco-friendly (Kai et al., 2011).

Patient have to bear the weight of monitor over prolonged period over the neck or on a belt underneath a shirt is burdensome and cumbersome, especially with many attached dangling wires as patients have to wear up to a minimum of 24 hours to record their heart rhythm. Besides, the main shortcoming of the previous Holter ECG is that it is a one way communication device in which no action can be immediately implement to the patient in emergency situation (Leijdekkers and Gay, 2006). Leads used in the ECG can be classified to 3 Leads, 5 Leads and 12 Leads depends on the purpose of monitoring. 3 Leads and 5 Leads are common used in continuous cardiac monitoring to identify the dysrhythmias whereas 12 Leads give the standard12 different views of heart which used to obtain specific diagnostic information (David et al., 2006), (Shade and Wesley, 2006).

2.3.2 Standard ECG Machine used in hospital

The most standard diagnostic equipment used by the hospital to detect any dysrhythmias. Figure 2.3 illustrate the ECG machine used in hospital. This type of ECG monitor used 12 leads to give a full view of heart activities of patient and important in diagnosis of the critical heart disease such as Ischemic Heart Diseaseand Coronary Heart disease. Cardiologist can diagnose the disease by print out the ECG vital on ECG paper for further analysis.

The weakness of using this ECG Machine is that patient are limited in movement as they required to lying in the bed and attach with dangling of wires to obtain the signal. Its limit the mobility of patient as it is bulky and hard to carry (Kai et al., 2011). This is troublesome and impractical for long terms use (Filipovic et al., 2013). Some of the dysrhythmias does not show any symptoms when the diagnostic process carry out, this always misleading the cardiologist to misdiagnosis (Luna, 2007). Sometimes, the cardiologist require to analysed the heart activity of patients when they doing exercise, this ECG machine cannot be used as it is not portable and disturb the patient's activities as the wires hinder the movement of patient.

2.3.3 Portable

The problems of using Holter are that patient has to regularly visit the hospital to updates the ECG data. Although the size of Holter is reduced, but it still consider large and burdensome for the patient who required to records their ECG signal with at least 24 hours (Kai et al., 2011). The weight of Holter together with the dangling wires can weigh up to one kilo which is a burden for patient. Besides, the Holter only allows recording function; it does not give an action when emergency situation occurs. The Holter ECG not able to analysed the signals on-line continuously since the cardiologist will be involved after patient update their data in clinics (Aliev et al., 2012).

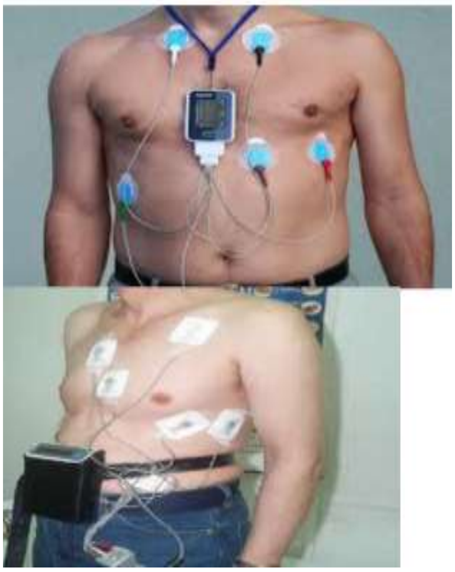

Figure 2.3 Holter ECG that wear over neck and waist

2.3.4 Handheld Heart Monitor

Figure 2.4 shows the handheld ECG monitor. Most of the handheld types of heart monitor monitoring using applications in smartphone by attaching with additional features to receive ECG signal instead of electrode pads. Normally the patient attach

the electrode pads few point surrounding the heart to receives electrical pulse from heart, but handheld heart monitor take the signal from fingertips.
The ECG data record in the handheld monitor usually able to transmit to smartphone using Bluetooth transmission as its low power consumption compared to WIFI which more suitable for long terms used. The power consume by Bluetooth is half compared to the WIFI due to its short transmission range. The research also shows that Bluetooth performance better than WIFI in short distance transmission (Friedman et al., 2013). Therefore, most of the heart monitor using Bluetooth to transmit data as low power consumption which suitable to receive ECG data continuously. One of the weaknesses of this invention is that it's only suitable to measure the instant heart rhythm which is impractical for 24 hours measurement.

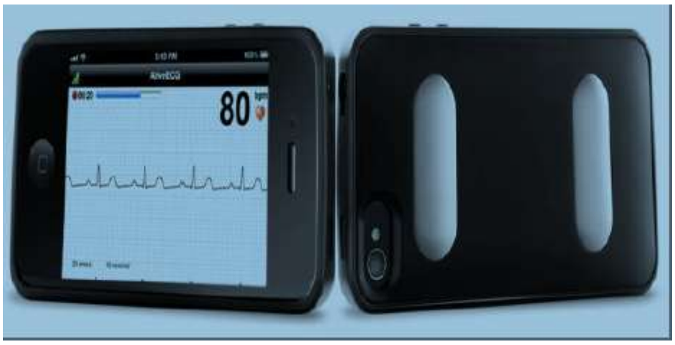

Figure 2.4 Handheld ECG monitor

2.3.5 Wrist Worn Heart Monitor

The hearts monitor which wear on the wrist of user

2.3.6 Wrist Worn Heart Monitor

The hearts monitor which wear on the wrist of user . This kind of monitor is small in size and will not cause the burden of the user. This monitor mostly used in sport to measure the heart rhythms during exercise. The shortcoming of this device is that it introduced noise due to motion artefact causing actual signal hard to identify(Kim et al., 2012). Therefore, it is not suitable to be used as a disease diagnostic tool as its accuracy is doubted.

2.3.7 Measure heart rate using applications in Smartphone

It function using the camera lens equip in the phone the measure the change of colour in fingertip to take the heart rate. Although this applications function as pulse oximeter, it provide the heart rates instead of full view of heart activities (Grimaldi et al., 2011).

Therefore, it is not a continuous heart rate monitor which is normally used in heart disease diagnosis.

3. CONCLUSION

To have presented LDK+, which is an improved version of the LDK scheme of Anjum. We added key revisions by incorporating the use of grid information into the previous dividing method, and we suggest key generation by combining the grid information. Thus, we solve the problem of insufficient numbers of nonces that can occur under the condition of communication interference and also consider key establishment and key revocation, as well as packet drop attack among other insider attacks. Through this simulation, we confirm that LDK+ has higher connectivity and a lower compromise ratio than LDK, which means that stability and security are improved. Moreover, through the hexagonal deployment of an AN arrangement, we show that network costs can be reduced without compromising the connectivity by decreasing the number of ANs. The Dijikstra algorithm used for finding the shortest path between source and anchor node. This algorithm reduces the energy consumption also.

REFERENCES

[1] Kemal Akkaya and Mohamed Younis. A survey on routing protocols for wireless sensor networks. Ad Hoc Networks, 3:325–349, 2005.

[2] D. F. Aranha and C. P. L. Gouvêa. RELIC is an Efficient Library for Cryptography. http://code.google.com/p/relic-toolkit/, August 2012.

[3] ARM Ltd. Cortex-M series. Website, September 2015. http://www.arm.com/products/processors/cortex-m.

[4] ARM Ltd. TrustZone. Website, September 2015. http://www.arm.com/products/processors/technologies/trustzone.

[5] Javier Barbarán, José A. Dianes, Manuel Díaz, Daniel Garrido, Luis Llopis, Ana Reyna, and Bartolomé Rubio. Programming wireless sensor networks applications using smepp: a case study. In Proceedings of 3rd ERCIM Workshop on eMobility, Enschede, Netherlands, May 2009.

[6] Eugen Berlin, Pablo Guerrero, Arthur Herzog, Daniel Jacobi, Kristof van Laerhoven, Alejandro Buchmann, and Bernt Schiele. Demo abstract: Whac-A-Bee – a sensor network game. In Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems, SenSys '09, pages 333–334, New York, USA, November 2009. ACM Press.

[7] John Bethencourt. Intro to bilinear maps. Slides, March 2006. http://www.cs.berkeley.edu/˜bethenco/bilinear_maps.pdf.

[8] John Bethencourt, Amit Sahai, and Brent Waters. Ciphertext-policy attribute based encryption. In IEEE Symposium on Security and Privacy, SP 2007, pages 321–334, Berkeley, CA, June 2007.

[9]BlueKrypt Cryptographic key length recommendation.Website,December2015. http://www.keylength.com.

[10] Dan Boneh and Matt Franklin. Identity-based encryption from the weil pairing. In Joe Kilian, editor, Advances in Cryptology (CRYPTO 2001), volume 2139 of Lecture Notes in Computer Science, pages 213–229. Springer Berlin / Heidelberg, 2001.

[11] Philippe Bonnet, Johannes Gehrke, and Praveen Seshadri. Towards sensor database systems. In Proceedings of the Second International Conference on Mobile Data Management, January 2001.

[12] Mirko Bordignon, Jayedur Rashid, Mathias Broxvall, and Alessandro Saffiotti. Seamless integration of robots and tiny embedded devices in a peis-ecology. In Proceedings of the IEEE/RSJ International Conference on Intelligent Robots and Systems, IROS 2007, San Diego, CA, 2007.