ISSN No. 0976-5697

Volume 6, No. 5, May - June 2015

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Cryptographic Key Exchange Scheme for Cloud Based Healthcare Monitoring

Lovepreet Kaur
Computer Science and Engg Deptt
CGC College of Engineering, Landran, India

Mr. Munish Mahajan
Computer Science and Engg Deptt
CGC College of Engineering Landran, India

Abstract: Healthcare monitoring sensor networks' based on cloud (C-HMSN) is collection of sensor nodes attached to patient's body and an each patient connecting through wireless connections. These systems set a stage to share medical applications, information and other types of data analysis in a fully automated way. Because these nodes are connected through wireless network with each other and base stations, it becomes a highly prone network to the hacking attacks .Patients' data confidentiality and communication safety are the main facets that would increase the belief of users in remote healthcare systems. HMSN are protected with automatic key management schemes. Current cryptographic key distribution and management techniques usually consume larger amount of energy and put high computational overheads on Wireless Sensor Nodes. The cryptographic keys are used on different communication levels of HMSN communications i.e. neighbor nodes, base stations and cluster heads. An effective corporate key management and distribution policy is required to maintain the security of the wireless sensor networks that permits only authorized applications/users to use the keys. In this paper, we will review the "Keep it Simple and Secure" corporate key management technique adaptable for the HMSNs by making it energy efficient.

Keywords: Healthcare monitoring; Cloud healthcare monitoring; key exchange; cloud security; Body Sensor Network; Wireless Body Area Network.

I. INTRODUCTION

Wireless Body Area Networks (WBANs) inhere of small and slight sensor nodes embedded, accompanied or attached on a patient body to collect various physiological changes to measure the patient's health condition regardless of their location. [31] Through gateway devices (smartphones, PDA, laptops etc.), it becomes possible to connect WBAN to the Internet. By connecting WBANs to the cloud enhances the development of cost-effective, efficient, scalable, and data-driven healthcare systems that provides the long-term health monitoring and analysis of patient's data under different environments. [2][16]Cloud computing refers to the supply of computing services over the Internet. Cloud services allow indivisibles to use hardware and software that are managed by third party at remote locations. [1][32] Examples of cloud services consist of online file storage, virtual office like Google Docs, social networking Websites, Email communication, backup services, and online business applications. [2][29]. The cloud computing platform permits access to information and computer resources from anywhere if network connection is available. Cloud computing provides a shared pool of assets, including space for data storage , networks, computer processing power, and specialized and general user applications[11] . By pooled assets, we mean that customers use from a pool of computing resources, normally in remote data centers [24].

The architecture uses sensor nodes attached to the human body that measures physiological values (PVs) and send these values to different servers located at the medical community cloud in a secure way. [2][30] The communication of sensors is made secure in WBANs and PVs are securely stored in the medical community cloud while preserving the confidentiality and privacy of personal data of patients [6]. Physicians, medical personnel and other consultants connected to the cloud will examine the patient's health on the basis of measured PV values and then carry out patient's treatment. [16] The overall architecture consists of sensors and a gateway for each patient (a smartphone, a PDA, tablet or a laptop). Data from these sensors is spurt wirelessly to a handheld device (a smartphone or tablet) and then gathered in the cloud by medical community [12] [27]. Authentication of the data generated by these devices is crucial to ensure proper analysis, traceability, and validation of affirmation. Patients, doctors, and medical staff, connected to the cloud, are liable to access information and resources with proper authorization in order to set out security and privacy of the system [15]. Information is made available to registered users in the hospital community cloud. As node communication is through wireless network with base station and each other, it becomes highly suspicious network to the security breach [20][21][28][32].

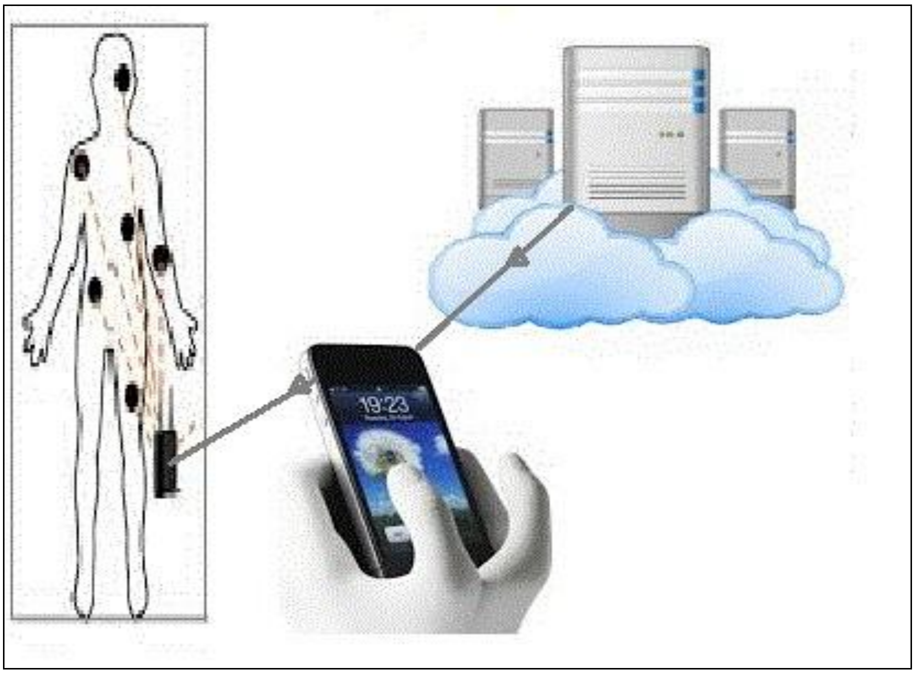

Figure1: Body Sensor with cloud based monitoring

II. SYSTEMS

A. Cloud-enabled wireless body area networks:

The status of patients can be monitored and tracked using plantable and non-plantable sensing devices. Security of WBAN sensors is very crucial to guarantee the confidentially and privacy of patient's personal data and for establishing secure communications between sensor and cloud servers [18] [19][25].

Venkata Subramanian et al. [30] proposed the EKG-based key agreement (EKA) scheme which deals with "plug-n-play" pattern to BSN security in which simply implanting sensors on the body can start secure data transmission and communication, without the requirement of any initialization activity such as pre-deployment etc. The analysis of scheme performed on real EKG data showed that resulting keys from EKA are: random, time variant (keys were generated on regular small intervals), EKG values were identical for a given subject and separate for different patients.

Wang et al. [32] proposed a new resource-aware BSN architecture for real- time patient monitoring, specifically for electrocardiogram data (ECG) [22][26] streaming and monitoring through wireless medium. For efficient monitoring of biomedical data [8], a cross-layer framework was developed dealing with unequal resource distribution. In this architecture, vital information is collected (like ECG data) and huge number of resources is allocated to protect it. Biomedical information processing and transmission are integrated under a common platform, where secure data transmission results in energy efficiency and minimum delay [5][7]. In the end, the authors presented an implantable, small, low-power ECG sensor node for real-time monitoring in biomedical applications.

Wan et al. [31] described that with the advent of mobile cloud computing, WBANs can be greatly embellished for huge healthcare applications. In this article, the authors studied a cloud based WBAN architecture and its introduction to healthcare systems. They highlight the successful methodologies for transmitting information to the cloud by using low energy consumption routing, resource allocation in cloud, security mechanisms and several technical issues and challenges to cloud enabled WBAN.

B. Secure key management based WBANs:

Very few works have been done for node authentication protocols in healthcare monitoring WSNs.

Ali et al. [2] proposed a combination of Merkle hash tree and network coding scheme for authentication lossy data (to recover the lost hash nodes in the tree) scheme. Secondly, a framework that (for optimization of given loss conditions and overhead) determines a baseline for use of coding to maximize the fraction, successfully verified data items by using the Gilbert model to simulate packet loss in a bodyworn sensor environment. Thirdly, the findings are validated using experimental traces of typical operating scenarios. Thus the proposed scheme has been low-cost and loss-resilient and has proved to be effective on almost 99% of data with as low as 5% overhead.

Khan et al. [13] described the security of cloud-based mobile healthcare framework. The authors have developed a multi-biometric based key generation scheme to secure inter-sensor communication for WBANs. They have also worked upon electronic medical records (EMRs) and secured them using the authentication scheme based on the key sharing process. Multi-biometric technique uses the fusion of two bio-metrics that measures physiological values namely ECG and EEG [17][23]. The motive behind the fusion of many biometric parameters is to increase the length of the key and to harden the security of key.

In [16], Lee et al. proposed an Elliptic Curve Cryptography (ECC) algorithm for key management to secure patient's medical data. ECC, a public key cryptography, has security solution for wireless networks due to the small key size and low computational overhead e.g. a 160-bit key in ECC is considered to be as secured as 1024-bit key in RSA. Elliptic Curve Diffie Hellman (ECDH) is a key exchange protocol that permits two parties to create and maintain a shared secret key that can be used for private key algorithms. Both parties exchange some public information with each other and each party using this public data and their own private data calculates the shared secret. The author's scheme is performed into three steps as setup, registration, verification and key exchange. The verification code was the patient's SIM card number aggregated with private key generated by the legal party. A message counter was applied at each authenticated message exchange process to prevent replay attack.

In [19], Mansour et al. proposed several multi-hop node authentication and key establishment protocols for WSNs. The key establishment solutions firstly use the sink as a trusted third party to setup a new key between two nodes in the network. Then, four protocols were proposed that uses other nodes in the network as trusted third parties in to create a new key. And the security of all solutions were proved using the automatic tool "Scyther" and all protocols were implemented and tested on TelosB nodes in to evaluate their execution time. Based on the delay of response reception measurements, it become possible to detect attack attempts from other nodes in the network.

In this paper [33], Zhou et al. considered a practical situation of cloud-enabled WBANs in m-healthcare networks where patients move among blocks outdoors and WBANs are more susceptible to attacks such as node compromise attack. For solving this problem of security, the authors introduced a privacy-preserving key management technique resilient to both location-based and time-based mobile attacks having mobile patients in same social group for hierarchical environment and among many social groups for distributed environment. The technique also preserves the confidentially of patient's identity, sensor deployment location by using blinding technique and infixing patient's body symmetric structure into Blom's symmetric key management technique. The privacy preserving key material updating is performed through the online server and the pairwise keys updated in key table results in energy saving for WBANs.

III. TECHNICAL CHALLENGES

For wearable healthcare monitoring devices to be indulged into the present healthcare system, health specialists must trust the data generated by these devices [10]. The data collected in the cloud should be trackable back to the originating device, and should not be intercepted by anyone, including authorized parties such as the patient or doctor or caregiver etc. [27] In the paragraphs below, we present some major issues to be kept in mind while designing wireless sensor networks for healthcare monitoring applications:

A. Reliability:

Healthcare applications enforce strict requirements of system reliability and delivery of data on time e.g., pulse oximetry applications, for measuring the levels of oxygen in blood of a person, must deliver at least one measurement value every 30s. Moreover, end users require measurements that are accurate and complete to be used in medical research. [2][3] The combination of end-to-end data delivery and quality properties are named as reliability of the system. Healthcare monitoring applications require high grade of reliability. [3]

A number of factors restrict the system's ability to provide reliability required by applications. First, medical areas, where these systems will be deployed, can have very rough environments for radiofrequency (RF) communications. [12] This roughness is due to environmental factors such as the presence of metal windows [14], doors as well as deliberate attempts to provide radiation shielding. [33] Moreover, devices that are based on 802.15.4 radios are more exposed to interference with Wi-Fi networks, cordless phones, and Bluetooth devices, all of which are largely used in hospitals. The impact of obstacles is infuriated by the fact that most wireless body area networks used today are low-power radios to achieve long battery lifetime of system.

B. Privacy and Security:

Wireless sensor networks examine the activities of an individual's daily life and provide data for analysis. However, WSNs can also pose circumstances to violate privacy [9]. So, the need of securing such systems is very essential as their adoption rate grows. Once the Personal Information Protection laws are specified by government, healthcare systems must implement these privacy rules and also be able to express data access policies for users [4].

C. Resource Scarcity:

In order to make tiny device work with reasonable battery lifetimes, wireless sensor nodes uses low-power components with moderate resources. [18] Use of limited power computation, communication components and energy resources in wireless sensor networks are the number of factors for challenging system design. The software design must satisfy these resource constraints. [14]

IV. DRAWBACKS OF EXISTING SYSTEMS

In today's world, body sensors are being used at a large to monitor the patients in their routine activity post- or pre-treatment. Wearable body sensors usually sends data to the medical databases directly through the wireless mediums (cellular networks, Wi-Fi, Zigbee, etc.). [15] The patients are informed by the medical database centers about their health on weekly or monthly basis by sending reports to their home or on their emails. [24] The healthcare monitoring data is aggregated on the servers and various types of algorithms are used for the healthcare data analysis. [16] The user privacy becomes the major concern in such healthcare monitoring systems.

We have found the following Major Drawbacks in the existing schemes:

a. In the existing scheme, the cloud server is the centralized key management server, which manages the secure connections between the medical database and the WBAN sensors. [3]
b. The key table is provided by the cloud server at the beginning of the connection making process, which is not a protected process. [1][3]
c. The WBAN sensors does not handle the automatic Data sharing cooperation between the cloud server and the WBAN sensor, hence it is not resilient against the connectivity breakage. [6]
d. The performance of the proposed key exchange is slightly better than the existing schemes in some cases (performance parameters like computational cost, etc.),

where it is under performed or almost similar in the case of probability of key exposure, which does not show the significant improve in the results. [6, 9]

e. Everything about the key exchange scheme, which includes the key-table generation, key verification, etc. are being provided by the cloud server, which may be hacked during the data exchange. [9]

These drawbacks can be mitigated using our proposed scheme. The new cooperative hybrid WBAN data privacy protection scheme is aimed at development of a resilient scheme against time-based and location-based mobile attacks.

V. SIGNIFICANCE OF KEY EXCHANGE

The key exchange mechanism has been designed to enhance the security of the wireless body area networks. The healthcare data privacy is very important. Any breach in the healthcare data exchange may alter the decision taken by the healthcare service provider to take any action against the health hazards. This type of model will be suitable for the low power heart beat sensors (also called Holter). An ideal security model for low power healthcare sensors must have the following properties:

a. The solution is intended to add the minimum possible network overhead.
b. The solution must have the quick response time during the key generation scheme.
c. The key generation scheme must follow the simple in key generation but difficult for guessing attacks and information reveal attacks.
d. The key transfer policy should offer the quick response mode, which adds the minimum amount of delay.
e. The key verification policy must be quick, which is only possible using the small or mid length security keys.
f. The key management policy must be efficient in terms of power consumption.
g. The key management policy must be efficient in terms of key memory storage. The light key table consumes the less amount of runtime memory on the healthcare sensor device, which directly affects the battery consumption.

VI. CONCLUSION

From the literature survey, this has been observed that the healthcare sensors require the security schemes in order to protect against the active and passive attacks on the healthcare networks. The existing security techniques have been studied in detail during the literature study. The shortcomings of the existing schemes have been studied in detail after analyzing the architecture of the existing models. The security loopholes have been found after evaluating the existing schemes. The model has been designed as the new robust security system for low power sensor networks in the healthcare networks and to provide hardened security with low power consumption. The expected outcome will be recorded for the key life cycle properties, such as key exposure, key connectivity, key verification time, key generation and key transfer time.

VII. FUTURE WORK

In future, we plan to enhance the proposed model to work more efficiently and quicker. The approach would be enhanced to protect against many types of attacks with one security solution. Also the elapsed time will be improved to increase the speed of the proposed approach.

VIII. REFERENCES

[1] Al-Fahoum, AS (2006) Quality assessment of ECG compression techniques using a wavelet-based diagnostic measure IEEE Transactions on Information Technology in Bio- medicine, 10, 182-191

[2] Ali, S T, Sivaraman, V, & Ostry, D (2014) Authentication of lossy data in body-sensor networks for cloud-based healthcare monitoring Future Generation Computer Systems, 35, 80-90

[3] ALSHAMALI, M AL-AQIL, 2011, "ECG compression using wavelet transform and particle swarm optimization", Journal of Medical Engineering & Technology, Vol 35, No 3–4, 149–153

[4] Al-Shrouf, A, Abo-Zahhad, M and Ahmed, SM, 2003, "A novel compression algorithm for electrocardiogram signals based on the linear prediction of the wavelet coefficients" Digital Signal Processing, 13, 604–622

[5] Anubhuti Khare, Manish Saxena, Vijay B Nerkar, 2011, "ECG Data Compression Using DWT", International Journal of Engineering and Advanced Technology (IJEAT), Volume-1, Issue-1

[6] Batista, LV, Melcher, EUK and Carvalho, LC (2001) Compression of ECG signals by optimized quantization of discrete cosine transform coefficients Medical Engineering & Physics, 23, 127-134

[7] Bendifallah, R Benzid and M Boulemden, 2011, "Improved ECG compression method using discrete cosine transform", 3191ELECTRONICS LETTERS Vol 47 No 2 DOI 101049/el2010

[8] Brechet, L, Lucas, MF, Doncarli, C and Farina, D (2007) Compression of biomedical signals with mother wavelet optimization and best-basis wavelet packet selection IEEE Transactions on Biomedical Engineering, 54, 2186-2192

[9] Cardenas-Barrera, JL and Lorenzo-Ginori, JV, 1999, "Mean-shape vector quantizer for ECG signal compression", IEEE Transactions on Biomedical Engineering, 46, 62 – 70

[10] Daubechies, I, 1988, "Orthonormal bases of compactly supported wavelets", Communications on Pure & Applied Mathematics, 41, 909–996

[11] Demir, B, Erturk, S and Urhan, O (2009) Improved quality multiple description 3D mesh coding with optimal filtering International Conference on Image Processing, Cairo, 7-10 November 2009, 3541-3544 Engineering (IJSCE), ISSN: 2231-2307, Volume-1, Issue-5

[12] He, Z and Mitra, SK (2000) Optimal quantization error feedback filter for wavelet image compression International Conference on Image Processing, 3, 166-169

[13] Khan, F A, Ali, A, Abbas, H, & Haldar, N A H (2014) A Cloud-based Healthcare Framework for Security and Patients' Data Privacy Using Wireless Body Area Networks Procedia Computer Science, 34, 511-517

[14] Ko, JeongGil, et al. "Wireless sensor networks for healthcare." *Proceedings of the IEEE* 98.11 (2010): 1947-1960.

[15] Lee, SJ, Kim, J and Lee, M (2011) A real-time ECG data compression and transmission algorithm for an e- health device IEEE Transactions on Biomedical Engineering, 58, 2448-2455_

[16] Lee, Y S, Alasaarela, E, & Lee, H (2014, February) Secure key management scheme based on ECC algorithm for patient's medical information in healthcare system In Information Networking (ICOIN), 2014 International Conference on (pp 453-457) IEEE

[17] M P S Chawla, 2009, "A comparative analysis of principal component and independent component techniques for electrocardiograms", Neural Comput & Applic, 18:539–556 DOI 101007/s00521-008-0195-1

[18] M Sabarimalai Manikandan, S Dandpat, Wavelet Threshold based ECG compression using USZZQ and Huffman coding of DSM, Science Direct Biomedical Signal Processing and Control 2006, pp 261-270

[19] Mansour, I, Chalhoub, G, & Lafourcade, P (2014) Evaluation of Secure Multi-Hop Node Authentication and Key Establishment Mechanisms for Wireless Sensor Networks Journal of Sensor and Actuator Networks, 3(3), 224-244

[20] Miaou, SG and Lin, CL (2002) A quality-on-demand algorithm for wavelet-based compression of electrocar-diogram signals IEEE Transactions on Biomedical Engineering, 49, 233-239

[21] Morteza Moazami-Goudarzi, Mohammad H Moradi, Ali Taheri, 2005, "Efficient Method for ECG Compression Using Two Dimensional Multiwavelet Transform", World Academy of Science, Engineering and Technology 2

[22] Nave G, and Cohen, A, 1993, "ECG compression using long-term Prediction", IEEE Transactions on Biomedical Engineering, 40, 877 –885

[23] Nielsen, M, Kamavuako, EN, Andersen, MM, Lucas MF and Farina, D (2006) Optimal wavelets for bio- medical signal compression Medical and Biological Engineering and Computing, 44, 561-568_

[24] Om Prakash, Vivek Chandra, Pushpendra Singh, 2012, "Design and Analysis of an efficient Technique for Compression of ECG Signal", International Journal of Soft Computing and

[25] Peng, X, Zhang, H, & Liu, J (2014) An ECG Compressed Sensing Method of Low Power Body Area Network TELKOMNIKA Indonesian Journal of Electrical Engineering, 12(1), 292-303

[26] S M AHMED, A F AL-AJLOUNI, M ABO-ZAHHAD, and B HARB, 2009, "ECG signal compression using combined modified discrete cosine and discrete wavelet transforms", Journal of Medical Engineering & Technology, Vol 33, No 1, 1–8

[27] S M AHMED, Q AL-ZOUBI, and M ABO-ZAHHAD, 2007, "A hybrid ECG compression algorithm based on singular value decomposition and discrete wavelet transform", Journal of Medical Engineering & Technology, Vol 31, No 1, 54 – 61

[28] S M S Jalaleddine, C G Hutchens, R D Strattan and W A Coberly 2009, "ECG Data Compression Techniques – A Unified Approach", IEEE Trans on Biomedical Eng, vol 37, 4, 329-341

[29] Velasco, MB, Roldan, FC, Llorente, JIG and Barner, KE (2004) ECG compression with retrieved quality guaranteed Electronics Letters, 40, 1466-1467

[30] Venkatasubramanian, K K, Banerjee, A, & Gupta, S K (2008, April) EKG-based key agreement in body sensor networks In INFOCOM Workshops 2008, IEEE (pp 1-6) IEEE

[31] Wan, J, Zou, C, Ullah, S, Lai, C F, Zhou, M, & Wang, X (2013) Cloud-enabled wireless body area networks for pervasive healthcare IEEE Network, 27(5), 56-61

[32] Wang, H, Peng, D, Wang, W, Sharif, H, Chen, H H, & Khoynezhad, A (2010) Resource-aware secure ECG healthcare monitoring through body sensor networks Wireless Communications, IEEE, 17(1), 12-19

[33] Zhou, J, Cao, Z, Dong, X, Xiong, N, & Vasilakos, A V (2014) 4S: A secure and privacy-preserving key management scheme for cloud-assisted wireless body area network in m-healthcare social networks Information Sciences