ISSN No. 0976-5697

Volume 6, No. 5, May - June 2015

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A Novel Lightweight Key Management Scheme for Patient Data Privacy on Body Sensor and Cloud based Healthcare Service

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

Manish Mahajan
Computer Science and Engg Deptt
CGC College of Engineering
Landran, India

Abstract: The healthcare networks consist of the wireless sensors to monitor the patient's health, hence called wireless body area networks (WBANs). The wireless sensors collect and transmit the health information to the healthcare management servers, which are usually hosted on the cloud platforms. The cloud platforms based healthcare management services offer high scalability and robustness in terms of response time, resource and data handling, but prone to various types of information leakage attacks due to the higher level of exposure to the outer world. The proposed model is based upon the secure tunnel based on randomized authentication & key management service, which is designed as the lightweight key management scheme for WBANs to protect the patient data privacy during the transmissions. The scheme aims at providing the higher level of security while keeping the battery consumption at the lowest possible level for the key management service.

Keywords: Data Transmission time; High Entropy Keys; Key Management; Patient data privacy; Randomized Key generation.

I. INTRODUCTION

All over the world, national health expenditures are experiencing massive pressure due to increase in age-related disabilities and severe medical conditions. The US makes $3.8 trillion, or 19.3% of its GDP expenditure on healthcare, and these costs are steeply rising every year. [3] A quality approach to rapidly cut costs is the arising pattern of e-health, which is a low-power network of bodyworn wireless sensor nodes. Wireless Body Area Networks (WBANs) is a network of small and tiny sensor nodes implanted on a patient body to obtain the physiological value measures of the body. The healthcare networks are growing across the world and positive results are being derived from such healthcare networks.

The healthcare networks are consisted of the wireless body sensors for live health monitoring and the healthcare database management servers. With the rise of cloud and its benefits in the management of infrastructure, flexibility and economics inspired many healthcare organizations to shift their healthcare records management service on the cloud platforms [17]. The cloud based healthcare service becomes more efficient as a higher volume of resources is always available for the applications hosted on the clouds, which can be utilized when the computational overhead increases due to the number of user requests or the internal application process execution.

A. Threats to data gathered by WBAN:

The WBAN [12] regularly works in situations with open access by different individuals (e.g., doctor's facility staff), which additionally suits aggressors. The open remote channel makes the information inclined to being eavesdropped, altered, and infused. In this article we principally concentrate on information storing and access, we show the dangers from the gadget perspective.

a. Dangers from gadget trade off: The sensor nodes in a WBAN are more sensitive to compromise, as they are generally simple to catch and not sealed [12]. In the event that an entire bit of information is straightforwardly encoded and put away in a hub alongside its encryption key, the tradeoff of this node will prompt the disclosure of information. Additionally, nearby servers may not be trustworthy, since there can be wicked individuals attempting to break into them to get patients' security data. They can either do the assault from the Internet, or basically go to the room where a patient is and sit tight for the opportunity to physically trade off a nearby server.

b. Dangers from system progress: The WBAN is very dynamic in nature. Because of incidental failure or malignant exercises, nodes may join or leave the system oftentimes. Node failure may occur because of absence of power. Assailants might effectively place faked sensors to disguise true ones, and could take away authentic nodes intentionally. The patient-related

information, if not having well maintained replica at multiple server's, could be lost effortlessly because of the system progress [12]. Additionally, false information could be infused or regarded as genuine because of absence of confirmation.

II. RELATED WORK

Protected and proficient pairwise key agreement schemes in sensor systems has been significantly envisioned, for example, q-composite scheme [3], E–G scheme [6], Liu's and Zhou's schemes centered around symmetric polynomials [14][19-22]. These plans require a pre-distribution key mechanism. Eschenauer et al. [6] presented a key-organizing scheme intended to fulfil both operational and security necessities of Distributed Sensor Network (DSN). The plan incorporates particular appropriation and renunciation of keys to sensor nodes and additionally node re-keying without generous processing and correspondence capacities.

It depends on probabilistic key offering among the nodes of an arbitrary diagram and uses straightforward conventions for imparted key revelation and way key foundation, and for key repudiation, re-keying, and incremental expansion of nodes. Zhou et al. [20] proposed a confident and privacy- preservative key management pattern for cloud- backed WBANs, resistant to time-based as well as place-based mobile attacks in m-healthcare social networks. The intended scheme holds the succeeding features: it resists mobile attacks to guard the secrecy of patient's identity, sensor placement and location secrecy in both categorised and dispersed environment. The cloud server outsources the computationally-escalated key material updating with proper protection scheme adopted against privacy that significantly results in energy-saving WBANs. The scheme structures the patient body's structure into Blom's method of symmetric key organization for delivering key updation materials, and it does not require any pre-installation or pre-distribution information at deployment.

Auspiciously, a large research work has been presented on implementing WBANs applications with integration to cloud [10][13][16-18] and building secure biometric-centred key interchange schemes in WBANs [9][21]. Khan et al. [9] presented a cloud-based secure system for versatile social insurance framework that spotlights inter-sensor correspondence security and in addition patients' information security and protection. The intended system customs multiple biometric values (face recognition, fingerprint, iris etc.) to produce a mutual key for inter-sensor communication and this is the only one complete framework and security solution for continuous monitoring healthcare system.

Fortunately, QRS detection approaches provide a precise use of ECG signals devising miscellaneous signal features, QRS morphologies, and heart rate variations [2][4][7]. Pan et al. [15] proposed a live monitoring algorithm for finding the QRS complexities in ECG signals. Slope, amplitude and width are the main attributes used for recognizing QRS complexes upon digital analyses of signal. Band pass filter were used to diminish false detections due to some disturbances or interferences in ECG signals. This filtering authorizes low thresholds and high detection sensitivity.

However, the hi-tech researches mainly focus on the security of WBAN using the key agreement in WBANs [5][9][12]. Ali et al. [1] proposed a low-cost solution against overhead constraints in data transmission in cloud. The authors employed a Merkle hash tree to perform digital signature and network coding for data verification to authenticate lossy data due to environmental and other overhead constraints. Huang et al. [8] exhibited a medicinal services checking construction modelling organized by three system levels which are giving pervasive, secure access to wearable sensor frameworks and remote sensor bits. This study united different remote methods and versatile encryption cryptography to advance an advantageous and secure administration for convenient and nonstop social insurance and environment observing. The authors proposed protected key management scheme built around elliptic curve cryptography (ECC) [11], divided into three segments as setup, enrolment, authentication and key interchange to protect the privacy of patient data. The identification code for authentication was the SIM card number of patient's smart phone aggregated with the private key created by the legal vendor.

III. PROPOSED SCHEME

The proposed scheme is specially proposed for wireless healthcare sensor networks. The wireless sensor nodes are battery operated devices, Hence, having limited power sources. The healthcare sensors or sensor networks sends data to the healthcare record management services via long distance wireless communication channels such as cellular networks or radio networks. The communication between the wireless body sensor and cloud based healthcare service passes from many insecure network ingress or egress points, where there is higher risk of the communication data being

exposed to the hackers. To protect the communication we are proposing a novel key exchange methods based upon the randomized key generation and management policy as the major improvement for the diffie-hellman scheme. Our scheme does not rely upon the key reversal or re-computational process, but is robust and rigid in nature, which does not allow any of the key guessing attacks. Such attacks do not let the sensor device to become hostile to the hackers and do not expose any information to the hackers. Our key scheme has been described in detailed below:

Algorithm 1: Randomized Function to generate random number

A. Firstly, set the arbitrary (random) number generator to make the outcomes in this case repeatable.

B. Create a radii value for each point in the sphere. These values are in the open interval, $(0,3)$, but are not uniformly distributed. The values have been created using the mathematic equation:

$$f(x) = 3 * \int_{1}^{1000000} random * \frac{1}{3}$$

C. Randomly select and concatenate the coordinates or values to create the OTP.

D. Return OTP

Key Management Policy:

Algorithm 2: Proposed Healthcare Authentication Protocol

1. The sensor nodes SN powers up
2. The sensor node SN initiates the sensing on the patient body where it has been deployed
3. The sensor node provides the pre-embedded patient ID and PIN to the cloud healthcare service using 1.

$$X = x_{i=1}^{k}, Y = y_{i=1}^{k} \quad (1)$$

$$Z = z_{i=1}^{k} \in \{0,1\}^{k} \quad (2)$$

4. The cloud healthcare service verifies the ID and PIN using 2.
5. If verification successful, the cloud healthcare server permits the sensor node SN to begin the data service
6. Otherwise, the cloud healthcare server denies the data from sensor node SN
7. The sensor node SN sends data channel request to cloud healthcare data management server
8. The cloud healthcare data management server sends a verification key
9. The sensor node reply with the corresponding verification acknowledgement key
10. The cloud healthcare server verifies the authentication key by matching the authentication against the verification key using 3 and 4.

$$l = l^{req}, \quad (3)$$

$$I(K_A;U) \le I^{adm}, \quad (4)$$

11. If key verification successful, the sensor node is updated with an acknowledgement to send the data and start the time counter for secure channel period
12. Otherwise, the sensor node is denied the data connection.
13. When the secure channel period time counter expires

i. The cloud healthcare server resends the verification key to the sensor node SN

ii. The sensor node reply with the corresponding verification acknowledgement key

iii. The cloud healthcare server verifies the authentication key by matching the authentication against the verification key

iv. If key verification successful, the sensor node is updated with an acknowledgement to send the data and start the time counter for secure channel period

v. Otherwise, the sensor node is denied the data connection.

14. Repeat the step 13 when the data communication is running.

IV. PERFORMANCE ANALYSIS

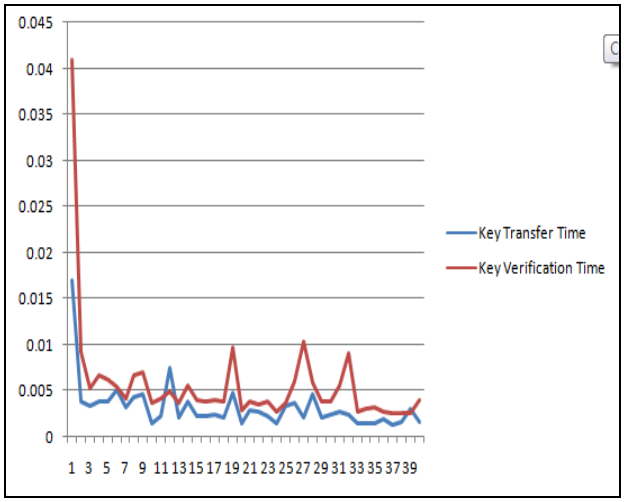

Figure 1: Time taken for key management scheme

The time taken for various procedures in the key exchange scheme has been recorded during the cloud based health monitoring sensor architecture simulation in the MATLAB simulator. The elapsed time has been recorded for various procedures: Time for Key generation, Time for key sharing or transfers, Time for key verification.

Entropy is the quantitative measure of disorder or randomness in a system. High entropy means higher security. Figure 6 shows the entropy comparison of the proposed scheme with ECG based scheme and EEG scheme. The proposed multi-biometric based scheme has high entropy as

compared to both ECG and EEG based schemes, which shows more randomness on average. Moreover, the length of the generated keys in is 128 bits and the proposed multi-biometric based scheme produces 128 bits.

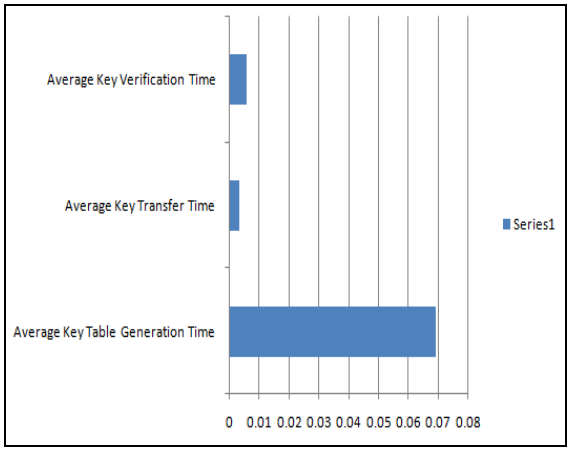

Figure 2: Bar Graph presentation of key generation, key transfer and verification schemes

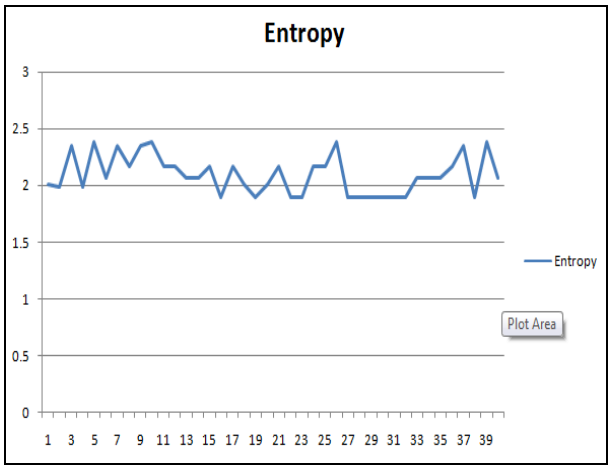

Figure 3: Entropy of the key generation scheme in cloud based healthcare sensor network

The data transmission time has been recorded for the sensor to Cloud healthcare application communication. The transmission time has been recorded on the real-time systems and has been considerably lower. The transmission time result indicates the effectiveness of the proposed system in efficiently delivering the data to the cloud based healthcare management applications.

a. Key Life-cycle Operations: Another threat is generated when the hackers try to change the key tables saved on the sensor nodes or to change the key generation policy by tweaking into the node software. The HCMN nodes carry a natural protection against software tweaking attack, because embedded system carry chip level programming which can't be changes on the fly. Also, the nodes will not flush or change the table on any of the hacking attempt by sending the data to the sensor nodes. The sensor nodes accept the data from the nodes replying with the reply keys. The key table is generated using high randomization based secure code generation technique, which does not hold any computational dependency on the base key. So the hacker can't gain the authorization and can't change key information table.

Table I. The time based analysis of the key lifecycle procedures

Data Index	Key Generation Time	Key Transfer	Key Verification
1	7.1399	2.923609346	3.416297625
2	8.139513989	2.026684854	2.047044406
3	7.233348557	2.132063017	2.095004555
4	3.452784155	2.027979864	2.036245348
5	3.70822252	2.035481684	2.086170405
6	3.368291291	2.030737358	2.085479515
7	3.300635889	2.031732407	2.037853848
8	3.322587613	2.029479202	2.0360998
9	3.269434362	2.020549418	2.090112348
10	3.352938707	2.036520118	2.035692543
11	3.47817913	2.070118067	2.088915303
12	3.47817913	2.070118067	4.369494867
13	3.47817913	2.070118067	4.226913627
14	3.47817913	2.070118067	4.456636063
15	3.47817913	2.070118067	4.209090913
16	3.47817913	2.070118067	4.094456415
17	3.47817913	2.070118067	4.101682067
18	3.47817913	2.070118067	4.074714046
19	3.47817913	2.070118067	4.159669213
20	3.47817913	2.070118067	4.050595886

The above table describes the time based analysis of the proposed model. The data has been transferred multiple times to the server from the healthcare sensor. The key lifecycle procedures have been evaluated on the basis of elapsed time during those processes. The key lifecycle procedures evaluated under this result analysis task are key verification time, key generation time and key transfer time. The key generation time is the time taken for the key selection from the key table and its encryption on the sender's side. The key selection is made randomly using the randomly generated index number, corresponding to which the key is selected from the first column in the key table.

The key transfer time is the time taken for the key transfer from sender to receiver, reply generation on the receiver side and key transfer from receiver side to sender side. The key transfer time signifies the communication cost

for the round trip time for the key exchange process. The verification time is the time taken by the sender to decrypt, match and to generate decision on the key matching process. Evaluating the key lifecycle also depends upon the latency caused by the internet communication channel. The experimental setup is based upon the client system on the local machine and the cloud healthcare system hosted on the online cloud hosting service. The real-time internet connection has been used for the communication between the healthcare sensor simulator on the client machine and the online health record management service. Hence, any latency caused by the internet directly affects the performance of the proposed model in terms of key transfer time.

The data updation time has also been recorded to signify the response time from the server to update the records. The data updation time includes the time taken for data generation, data transfer, update query and response reply from the server side. The updation time has been recorded on each data update interval during the simulation environment. The nineteen update intervals have been evaluated in the following table, which also involves the latency caused by the online cloud healthcare record management service.

Table 2. The data update interval evaluation on the basis of elapsed time

Update Interval	Elapsed Time on each update interval
1	7.095176
2	3.314872
3	3.556126
4	3.222195
5	3.190924
6	3.228668
7	3.209415
8	3.293027
9	3.399302
10	3.211423
11	3.022632
12	3.259632
13	2.93297
14	2.947099
15	2.915975
16	2.907033
17	2.939347
18	2.901044
19	2.900924

V. CONCLUSIONS

The proposed model has been designed for the cloud based healthcare management networks. The proposed model is aimed at the data privacy and information leakage protection by building the secure channel between the WBAN sensor and Cloud based healthcare management service. The secure tunnel ensures the security of the proposed model by using the lightweight key management scheme with lightweight encryption to ensure the data privacy and communication link security between the body sensor and cloud based healthcare management service. The proposed model performance has been measured using various parameters. The entropy has been recorded at higher level which indicates the effectiveness of key generation model by estimating the uniqueness of the keys. Also the key verification process time has been recorded at lower levels which ensure the effectiveness of the proposed model.

VI. REFERENCES

[1] Ali, Syed Taha, Vijay Sivaraman, and Diethelm Ostry. "Authentication of lossy data in body-sensor networks for cloud-based healthcare monitoring." Future Generation Computer Systems 35 (2014): 80-90. GG

[2] Arzeno, Natalia M., Zhi-De Deng, and Chi-Sang Poon. "Analysis of first-derivative based QRS detection algorithms." Biomedical Engineering, IEEE Transactions on 55.2 (2008): 478-484. QQ

[3] Chan, Haowen, Adrian Perrig, and Dawn Song. "Random key pre-distribution schemes for sensor networks." Security and Privacy, 2003. Proceedings. 2003 Symposium on. IEEE, 2003.

[4] Debbabi, Nehla, Sadok El Asmi, and Hichem Arfa. "Correction of ECG baseline wander application to the Pan & Tompkins QRS detection algorithm." I/V Communications and Mobile Network (ISVC), 2010 5th International Symposium on. IEEE, 2010.

[5] Du, Xiaojiang, et al. "An effective key management scheme for heterogeneous sensor networks." Ad Hoc Networks 5.1 (2007): 24-34. MM

[6] Eschenauer, Laurent, and Virgil D. Gligor. "A key-management scheme for distributed sensor networks." Proceedings of the 9th ACM conference on Computer and communications security. ACM, 2002. NN

[7] Friesen, Gary M., et al. "A comparison of the noise sensitivity of nine QRS detection algorithms." Biomedical Engineering, IEEE Transactions on 37.1 (1990): 85-98.

[8] Huang, Yueh-Min, et al. "Pervasive, secure access to a hierarchical sensor-based healthcare monitoring architecture

in wireless heterogeneous networks."Selected Areas in Communications, IEEE Journal on 27.4 (2009): 400-411.CC

[9] Khan, Farrukh Aslam, et al. "A Cloud-based Healthcare Framework for Security and Patients' Data Privacy Using Wireless Body Area Networks." Procedia Computer Science 34 (2014): 511-517. HH

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

[11] Lee, Young Sil, Esko Alasaarela, and HoonJae Lee. "Secure key management scheme based on ECC algorithm for patient's medical information in healthcare system." Information Networking (ICOIN), 2014 International Conference on. IEEE, 2014. AA

[12] Li, Ming, Wenjing Lou, and Kui Ren. "Data security and privacy in wireless body area networks." Wireless Communications, IEEE 17.1 (2010): 51-58. EE

[13] Li, Yang, Li Guo, and Yike Guo. "Enabling Health Monitoring as a Service in the Cloud." JJ

[14] Lu, Rongxing, et al. "A secure handshake scheme with symptoms-matching for mhealthcare social network." Mobile Networks and Applications 16.6 (2011): 683-694.

[15] Pan, Jiapu, and Willis J. Tompkins. "A real-time QRS detection algorithm." Biomedical Engineering, IEEE Transactions on3 (1985): 230-236.

[16] Wan, Jiafu, et al. "Cloud-enabled wireless body area networks for pervasive healthcare."Network, IEEE27.5 (2013): 56-61.

[17] Zhang, Jiang, and Zhenfeng Zhang. "Secure and efficient data-sharing in clouds."Concurrency and Computation: Practice and Experience(2014).

[18] Zhang, Rui, and Ling Liu. "Security models and requirements for healthcare application clouds."Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on. IEEE, 2010.

[19] Zhou, Jun, and Mingxing He. "An improved distributed key management scheme in wireless sensor networks."Information Security Applications. Springer Berlin Heidelberg, 2009. 305-319.

[20] Zhou, Jun, et al. "4S: A secure and privacy-preserving key management scheme for cloud-assisted wireless body area network in m-healthcare social networks."Information Sciences(2014).

[21] Zhou, Jun, Zhenfu Cao, and Xiaolei Dong. "BDK: secure and efficient biometric based deterministic key agreement in wireless body area networks. "Proceedings of the 8th International Conference on Body Area Networks. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2013.

[22] Zhou, Yun, and Yuguang Fang. "Scalable and deterministic key agreement for large scale networks."Wireless Communications, IEEE Transactions on6.12 (2007): 4366-4373.