International Journal On Engineering Technology and Sciences – IJETS™
ISSN(P): 2349-3968, ISSN (O): 2349-3976
Volume IV, Issue VIII, August - 2017

# Construction of Health Care Monitoring Framework with Secure WBAN Data Communication

Mrs. K. Gayathri, MPhil., Research Scholar,
Mrs. V. Shanmuga Priya, MCA., MPhil., (PhD), Asst. Professor, Department of CS,
PGP College of Arts and Science. Namakkal, Tamilnadu, India,

**Abstract**

The health care monitoring framework is build with the support of the smart phones and sensor devices. The mobile health services are used for the health care monitoring framework. The sensor devices are employed to monitor the blood pressure, Oxygen level and body temperature information. The Wireless Body Area Networks (WBAN) is build with the sensor devices. The radio frequency mediums are adapted for the data communication between the smart phones and sensor devices. The Device to Device (D2D) data communication security applications are build with authentication, confidentiality and data integrity operations.

The mobile health monitoring applications are build with Light-weight and Robust Security-Aware (LRSA) D2D-assist data transmission protocol. The data transmission security is provided with the Certificateless Generalized Signcryption (CLGSC) technique. The Signcryption, signature and encryption are integrated in the CLGSC technique. The Network Manager (NM), WBAN client and Medical Service Provider (MSP) are the three elements used in the health care monitoring services. The initialization and key generation tasks are carried out by the Network Manager for the WBAN clients and Medical Service Providers.

The optimal relay discovery and data forwarding (ORF-DF) models are combined in the secure WBAN data communication based health care monitoring framework. The data aggregation based query model is integrated in the health care monitoring framework. The event detection based decision support model is combined in the system. The data forwarding operations are build with priority factors. The security model is improved with node anonymization and data privacy methods. The data transmission overhead is reduced with the data cache and replication based methods.

**Index Terms : Wireless Body Area Networks (WBAN), Mobile Health Services, Cryptography, Digital Signature and Signcryption**

## 1. Introduction

Ubiquitous healthcare is an emerging technology that promises increases in efficiency, accuracy and availability of medical treatment due to the recent advances in wireless communication and in electronics offering small and intelligent sensors able to be used on, around, in or implanted in the human body. In this context, Wireless Body area networks (WBANs) constitute an active field of research and development as it offers the potential of great improvement in the delivery and monitoring of healthcare. WBANs consist of a number of heterogeneous biological sensors. These sensors are placed in different parts of the body and can be wearable or implanted under the user skin. Each of them has specific requirements and is used for different missions. These devices are used for measuring changes in a patient vital signs and detecting emotions or human statuses, such as fear, stress, happiness, etc. They communicate with a special coordinator node is generally less energy constrained and has more processing capacities. It is responsible for sending biological signals of the patient to medical doctor in order to provide real time medical diagnostic and allow him to take the right decisions.

The WBAN common architecture consists of three tiers communications: Intra-BAN communications, Inter-BAN communications and beyond-BAN communications. Intra-BAN communications denote communications among wireless body sensors and the master node of the WBAN. Inter-BAN communications involve communications between the master node and personal devices such as notebooks, home service robots and so on. The beyond-BAN tier connects the personal device to the Internet. Communications between different parts is sup-ported by several technologies, such as Bluetooth, IEEE 802.15.4. IEEE 802.15.6 was designed especially for WBAN applications while responding to the majority of their requirements. It looks less performing in some cases in comparison with other technologies supporting WBAN. Wi-Fi, Bluetooth and mobile

networks can be solutions for implementing WBAN applications, since each technology offers specific characteristics, allowing it to meet the constraints of some applications. In fact, WBAN applications cover numerous fields in order to improve the users quality of life. These applications can be categorized mainly according to whether they are used in medical field or in non-medical field. Non-medical applications include motion and gestures detection for interactive gaming and fitness monitoring applications, cognitive and emotional recognition for driving assistance or social interactions and medical assistance in disaster events, like terrorist attacks, earthquakes and bush fires. Medical applications comprise healthcare solutions for aging and diseased populations mainly. Typical examples include the early detection, prevention and monitoring of diseases, elderly assistance at home, rehabilitation after surgeries, biofeedback applications controls emotional states and assisted living applications which improve the quality of life for people with disabilities.

## 2. Related Works

Several research works has been carried out for securing the medical inf network [4], [6]. Cryptographic keys are generated from the electrocardiogram (ECG) signals and are used for encrypting the communication between pair of sensor nodes in BSN. In this work, the ECG values are obtained for a specific interval of the signal and the fast Fourier transform is employed to extract the coefficients[3]. Then feature vectors are generated based on these coefficients that are used for generation of keys. The derived key is then used to encrypt the communication. The aim of this work is to secure the inter sensor communication [12]. The key generated using this approach is different for various people since the ECG value is different for each people.

In [8] a two-tier authentication scheme is used for securing healthcare information's of the BSN. Security is achieved in two phases: In the first phase a unique key is generated in a decentralized manner and is used to encrypt the information. In the second phase, the key is utilized as a session key for authenticating data aggregation node from the sensor node [7]. This approach provides security, authorization and confidentiality of the healthcare information.

A hybrid authenticated key agreement through rekeying has been proposed for body sensor networks [9]. The approach is based on symmetric cryptography and elliptic curve for the purpose of key agreement. [10] uses a Elliptic Curve Cryptography (ECC) for generating keys that is used to encrypt the communication between the sensor node and the base station. In this approach, RC5 block cipher is used for encryption and decryption process. This process ensures data integrity and confidentiality.

In [11] security in body sensor network is achieved by employing cryptographic techniques. Here, the ECG signals are utilized to generate keys. In this work, encryption is performed using Advanced Encryption Standard (AES). The Public Key Cryptography (PKC) with re-keying approach has been utilized for key establishment. Here, RSA and DHECC parameters are utilized for key-agreement protocol that provides rekeying features. A particular routing algorithm has been used in the agreement phase for achieving resilience, scalability and memory efficiency. But the RSA and DHECC as well as PKC increases the computational cost of the BSN.

A novel chaos based encryption technique has been developed [1] for avoiding unauthorized access of ECG signal in inter- body sensor network communication. Here true random numbers are used for deriving the chaos key. This approach uses Diffie Hellman key exchange algorithm for exchanging the key between the node and the base station.

In [2] EKG is used as physiological measures to generate cryptographic keys for securing inter sensor communication. First the communicating sensor nodes sense EKG values and then hashing and watermarking approaches are applied to exchange values to generate public key for communication. [5] also utilizes biometric measures as symmetric keys as they as random. In this framework, key refreshment concept is utilized where the server provides key refreshment schedule to all the nodes of the BSN. This schedule exchanges the key allocated to it for communication. Here three keys namely, communication key, administrative key and basic key are utilized.

## 3. WBAN Based Health Services

The Mobile-Health (M-Health) system has been envisioned as a promising approach to improving healthcare quality and save lives in the aging society. In MHealth systems, the Personal Health Information (PHI) is collected by Body Area Network (BAN) and aggregated by smartphone. Then the data is sent to the healthcare center via cellular networks. With the increasing popularity of

mobile healthcare, the medical data sent to base stations may aggravate the already over-burden cellular networks. Fortunately, Device-to-Device (D2D) communications are employed to be an advantageous solution to meet with the explosive demanding of spectrum because they can be operated on the same time/frequency resources over short distances. Consequently, The PHI data through D2D communications Is adapted for M-Health systems.

Due to the intrinsically open nature of wireless communications and dynamics of cellular networks, D2D communications are vulnerable to security attacks such as eavesdropping, fake message, privacy violation, etc. Currently, security for M-Health systems has attracted extensive attentions. Most of these works mainly focus on either anonymous authentication or privacy-preserving issues while ignoring the security during data transmission. Lin et al firstly consider this problem by proposing a strong privacy preserving scheme against global eavesdropping for eHealth systems. These are pioneer works on security-aware data transmission for M-Health systems while they don't take into account the D2D-assist data transmission scenarios.

Actually, security-aware D2D-assist PHI transmission for M-Health systems is challenging due to the privacy sensitive characteristics of PHI data and the insecure D2D transmission. Specifically, the protocol design should consider the following issues: i) How to guarantee the PHI not to be accessed by the relays while the relays are able to judge whether the data is altered by attackers? ii) How to achieve mutual authentication between the source client of the data and its intended physician without interaction? iii) The protocol should be light weight in the sense that the mobile terminals have energy and storage constraints, i.e., the computational and communication cost should be low. iv) The protocol should be robust enough to face the threat when part of the keys is exposed, i.e., the PHI remains secure even if part of the keys is disclosed.

The Certificateless public key cryptography (CLPKC) is used to achieve the designed security objectives. In CLPKC, the users' private key is not generated by the Key Generator Center (KGC) alone but a combination of the contributions of the KGC and the user. The KGC does not know the user's private key but can authenticate its public key. In this way, the key escrow problem of the ID-based public key cryptography is solved. Additionally, the CLPKC avoids the problem of certificate revocation, storage and distribution in certificate-based public key cryptography. Generally, the CLPKC has three techniques, i.e., Certificateless signature, certificateless encryption and certificateless signcryption. The three techniques are usually realized by three different algorithms and are applicable in different application scenarios.

In order to adaptively work as a signcryption scheme, a signature scheme, or an encryption scheme with only one algorithm, a certificateless generalized signcryption (CLGSC) scheme is put forward. However, all the existing CLGSC schemes are realized with pairing operations, which is time consuming and has low computational efficiency. The CLGSC scheme is low in time consumption cost and proven to be secure in confidentiality and unforgeability.

The new CLGSC algorithm can operate on three modes: signcryption mode, signature mode, or encryption mode adaptively. CLGSC is applied to design a light-weight and robust security-aware (LRSA) D2D-assist data transmission protocol for M-Health systems. PHI data is encapsulated with signcryption mode and the source's identity is encrypted with the encryption mode by the source client, thus achieving data confidentiality and integrity, mutual authentication and contextual privacy. A session key is introduced in the signcryption algorithm to enhance the security strength. And the session key is updated by a secure hash function at the end of each transmission session to achieve forward security. The source client and all the relays sign on the encrypted data to guarantee data integrity. The LRSA protocol can also achieve anonymity and unlinkability by using the pseudo identity and a random number in the ciphertext of the identity.

The efficient certificateless generalized signcryption (CLGSC) scheme is adapted for the security process. The CLGSC is built based on Elliptic Curved Discrete Logarithm Problem (ECDLP) and implemented without pairing. It has the lowest computational cost comparing with the existing CLGSC schemes. Moreover, it is proven to achieve confidentiality and unforgeability in the random oracle model (ROM) under the Discrete Logarithm Problem (DLP) and CDHP (Computational Diffie-Hellman Problem) assumption.

The lightweight and robust security-aware (LRSA) D2D-assist data transmission protocol is build for M-Health systems based on the CLGSC scheme. LRSA achieves data confidentiality and

integrity, mutual authentication and contextual privacy by using the CLGSC scheme. Furthermore, anonymity and unlinkability are simultaneously realized by using the pseudo identity and choosing different random numbers at different sessions. Additionally, LRSA has the characteristics of forward security with hash chain of the session key.

The security properties of the LRSA is analyzed and compare it with the other protocols terms of data confidentiality and integrity, mutual authentication, anonymity, unlinkability, forward security and ontextual privacy. The computational overhead and communication overhead are compared between the CLGSC algorithm and the other Certificateless generalized signcryption schemes.

## 4. Problem Statement

The Light-weight and Robust Security-Aware (LRSA) D2D-assist data transmission protocol is constructed for M-Health systems. The Certificateless Generalized Signcryption (CLGSC) technique is employed to provide the security for the D2D data communication. The CLGSC scheme integrates the signcryption, signature and encryption with in single channel. The mobile health system is build with three elements. They are Network Manager (NM), WBAN Client and Medical Service Provider. The network manager handles the initialization and key generation operations for the WBAN clients and Medical Service Providers. The WBAN client collects and transfers the health information from the patients. The Medical Service Provider (MSP) analyzes the patient health information collected from the WBAN clients. The following security issues are discovered from the current mobile health services. Relay node selection and data transmission scheduling is not optimized. Data and node level privacy is not provided. Query processing and event detection operations are not supported. Data transmission priority levels are not considered.

## 5. Secured Healthcare Monitoring Framework

The mobile health service security scheme is enhanced with optimal relay selection and data forwarding policies. The medical data aggregation based query processing is supported in the system. Event detection and decision support operations are integrated with the system. The Priority level based data forwarding, data cache and replica schemes are integrated to support efficient data communication tasks.The M-Health services are build with D2D data communication security models. Relay selection and query processing operations are improved with data forwarding schemes. Node anonymization and data privacy features are combined to improve the security process. The M-Health system is divided into six major modules. They are Medical Service Provider, WBAN Client, Network Manager, Relay selection and data forwarding process, Privacy and security services and Query Management.

The medical service provider manages the patient health information and health care services. The patient details are collected by the WBAN client application. The network manager is an interface between the WBAN client and medical service provider. Relay selection and data forwarding module is designed to choose the relay node for data transmission process. Node and data values are protected in the privacy and security process. The query management module handles the query processing and event detection operations.

The Medical Service Provider (MSP) application is build to handle the patient health management services. Patient health information are collected from the Wireless Body Area Network (WBAN) clients. Patient health levels and criticality conditions are continuously monitored by the Medical Service Providers. Medical assistance and services are provided with reference to the patient health information. The Wireless Body Area Network (WBAN) is constructed with the support of the small sensors used for the health monitoring process. The blood pressure, Oxygen level and body temperature information are observed and maintained by the WBAN clients. The health information are transferred to the Medical Service Provider for health care analysis. Data aggregation and event detection operations are carried out through the WBAN clients.

The Network Manager (NM) is the interface between the Medical Service Providers (MSP) and WBAN clients. The network manager maintains the information about the Medical Service Provider and WBAN clients. Initialization and key generation operations are carried out under the Network Manager environment. The key values are distributed to the Medical Service Providers and WBAN clients. The relay nodes are used to manage the data retransmission operation. The optimal relay selection process is carried out with traffic level and coverage details. The data forwarding process is handled with priority information. Data cache and replica schemes are also adapted to improve the data forwarding process.

The Light-weight and Robust Security-Aware (LRSA) D2D-assist data transmission protocol is used for the secure communication process. The data transmission process is protected with Certificateless Generalized Signcryption (CLGSC) technique. Node and data level privacy is provided in the system. The Advanced Encryption Standard (AES), RSA and Secure Hashing Algorithm (SHA) are employed in the data security process. The query management process is adapted to support medical data access process. Data aggregation based query process provides the health data summary details. Event detection and decision operations are managed under the query management process. The query request and response values are protected with privacy and security features.

## 6. Conclusion and Future work

The Mobile Health (M-Health) services are provided with Wireless Body Area Network (WBAN) and Smart phone technologies. M-Health systems are protected with Light-weight and Robust Security-Aware (LRSA) Device to Device (D2D) assist data transmission protocol. The M-Health services are improved with aggregation based query process, optimal relay selection and data forwarding scheme. Priority based data forwarding and event detection operations are supported with data privacy and security features. The Medical Health (M-Health) services are build with lightweight security based Device to Device (D2D) communication process. The optimal relay selection process improves the data forwarding process. Automatic and request based data transmission operations are supported in the system. Data transmission process is improved with cache and replica concepts. The mobile health services data processing load can be managed with the support of the cloud resources. The system can be upgraded with energy and bandwidth management techniques.

## References

[1] Sufi, F., Han, F., Khalil, I., & Hu, J. (2010). A chaos-based encryption technique to protect ECG packets for time critical telecardiology applications. Security and Communication Networks.

[2] Aftab, A., & Farrukh, A. K. (2010). An improved EKG-based key agreement scheme for body area networks. Proceedings of the International Conference on Information Security and Assurance.

[3] Haipeng Peng, Ye Tian, J¨urgen Kurths, Lixiang Li, Yixian Yang and Daoshun W, "Secure and Energy-Efficient Data Transmission System Based on Chaotic Compressive Sensing in Body-to-Body Networks", IEEE Transactions On Biomedical Circuits And Systems, 2017.

[4] Lewko, A., Okamoto, T., Sahai, A., Takashima, K., & Waters, B. (2010). Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. Advances in Cryptology Eurocrypt.

[5] Raazi, S. M. K., & Lee, H. (2009). BARI: A distributed key management approach for wireless body area networks. Proceedings of the International Conference on Computational Intelligence and Security.

[6] Lee, P. Y. D, & H. J. Lee. (2010). Secure health monitoring using medical wireless sensor networks. Proceedings of the 6th International Conference on Networked Computing and Advanced Information Management.

[7] Hongguang Zhang, Kai Liu, Weijian Kong, Fei Tian, Ti Wang and Qi Chen, "A Mobile Health Solution for Chronic Disease Management at Retail Pharmacy", 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), IEEE, 2016.

[8] Kanjee, M. R., Divi, K., & Liu, H. (2010). A two-tiered authentication and encryption scheme in secure healthcare sensor networks. Proceedings of the International Conference on Information Assurance and Security.

[9] Amin, N., Asad, M. N., & Chaudhry, S. A. (2012). An authenticated key agreement with rekeying for secured body sensor networks based on hybrid cryptosystem. Proceedings of the IEEE International Conference on Networking, Sensing and Control.

[10] Malasri, K., & Wang, L. (2009). Design and implementation of a secure wireless mote-based medical sensor network. Sensors.

[11] Liu, J. W., Zhang, Z. H., Rong, S., & Kwak, K. S. (2012). Certificateless remote anonymous authentication schemes for wireless body area networks. Proceedings of the IEEE International Conference on Communications (ICC).

[12] A. Siva Sangari and J. Martin Leo Manickam, "Secure Communication over BSN Using Modified Feather Light Weight Block (MFLB) Cipher Encryption", Journal of Software, Volume 10, Number 8, August 2015.