Technical Journal, University of Engineering and Technology (UET) Taxila, Pakistan Vol. 23 No. 2-2018
ISSN:1813-1786 (Print) 2313-7770 (Online)

Securing Data Communication in Wireless Body Area Networks Using Digital Signatures

M. Anwar[1], A. H. Abdullah[2], R. A. Butt[3], M. W. Ashraf[4], K. N. Qureshi[5], F. Ullah[6]

[1,2]*Faculty of Computing, Universiti Teknologi Malaysia, Malaysia*
[3]*Telecommunication Engineering Department, NED UET, Karachi, Pakistan*
[4]*Computer Engineering Department, Bahauddin Zakariya University, Multan, Pakistan*
[5]*Computer Science Department, Bahria University Islamabad, Pakistan*
[6]*Computer Science Department and IT, Sarhad University of Science and IT, Peshawar, Pakistan*
[1]anwer.mirza@gmail.com

Abstract-Wireless Body Area Networks (WBANs) is an evolving technology for healthcare applications. It provides the opportunity to medical service providers to remotely monitor the health status of their patients on real time basis. In WBANs, sensor nodes collects data of vital signs and send to the medical server for further analysis. Since this data contains life-critical sensitive information so the security, privacy and safety of this data is a main challenge. In this paper, we highlight the major issues and challenges related to data security and privacy in WBANs. Further we propose a data hybrid method named D-Sign for encrypting and decrypting using digital signatures. We also analyze the performance of the proposed method against the state-of-the-art mechanisms aimed to ensure the security and privacy in WBANs.

Keywords-Wireless Body Area Networks, Security and Privacy

I. Introduction

The advancement in information and communication technology (ICT) brought revolution in today's human life. Wireless Sensor Networks (WSNs) are one of the most influential advancement in ICT. WSNs are type of wireless networks based on small distributed sensors to collect and monitor data for different applications [i], [ii]. WSN technology offers extensive applications which can be used in military, engineering, agriculture, biomedical, urban management, environment monitoring, disaster recovery and other various fields [iii]. To make more advancement in WSN specially for healthcare, the researchers from ICT and medical science introduced Wireless Body Area Networks (WBANs) [iv]. WBANs are the collection of tiny sensor nodes and actuators placed on or in the human body. These sensor nodes are of two types; on-body and in-body (implantable). The sensor nodes measure the various body parameters whereas the actuators act according to the received data from other sensor nodes [v]. In addition, Body Node Coordinator act as control unit to collect data from sensor nodes and transmit to the medical server using wireless communication link [vi]. WBAN network architecture is categorized into two main types: intra-WBAN and beyond-WBAN. The intra-WBAN refers to a network in which the sensor nodes placed on or near the surface of human body. On the other hand, the beyond WBAN is designed as a gateway node bridges the connection between intra and inter WBAN. The network architecture of WBAN is shown in Fig.1. The sensor nodes send their sensory data to body coordinator in intra-WBAN. As this data contains life-critical and sensitive information therefore, the security, privacy and safety of this data is very inevitable [vii]. In this paper, we highlight the major issues and challenges related to data security and privacy in WBANs, and discuss state-of-the-art mechanisms to ensure the security and privacy in WBANs.

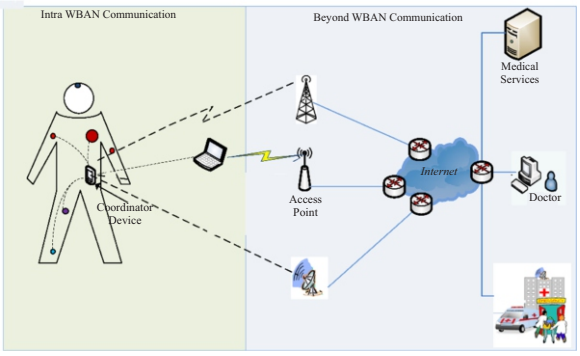

Fig.1. Architecture of WBAN [viii]

II. Security and Privacy Challenges in WBANs

Since WBAN sensors generates life-critical sensitive information so security and privacy is one of the significant factor to design any application for WBANs. The patient data is based on important facts and critical to diagnose the diseases. If this data is not correct or corrupted by means of any security flaw, then

the impact of this tempering cause of ineffective treatment of patient and threat for their life. The patient data is private for and need to address privacy concerns [ix]. Every country has own security policies and based on their rules and laws. To ensure the security and privacy for WBANs data, there are many difficulties due to various security threats. Basically, the security is divided into two broad categories including physical security of data and communication security. In physical security, the unauthorized data access, media distribution threat, faulty hardware, and software attacks such as worms, virus and spyware are included. On the other hand, in communication security threats are data eavesdropping, mobile-to-mobile attacks, spoofing, activity tracking and scrambling attacks[x-xi]. In WBANs, various types of attacks are noticed such as data impairment, data disclosure, sinkhole, route spoofing, flooding threats and denial of services (DOS) attacks.[xii].

III. Existing Solutions for Security in WBANs

There are various types of security mechanism have been developed based on encryption, decryption, verifying signature. The sensors limited energy also prohibits the complex and difficult security mechanism. The WBANs are more energy and memory constrained compared with WSN. Most of WSN bases routing protocols are not suitable for WBANs [vi] . The WBANs security requirements are security and privacy of patient data to ensure the data communication with less energy consumption. In this context, data confidentiality, integrity and availability are key requirements in WBANs [xii]. Confidentiality refers to keep the data secure during storage in server. The data integrity refers to keep the data from unauthorized changes during data storage and transmission. The data availability refers to data is available in its original form to the genuine users [xiii]. In this section we provide the state-of-the-art solutions proposed for security and privacy in WBANs. This section is organize by studying existing methods that how they address issues related to security and privacy in WBAN.

A. Biometric Authentication Methods

In [xiv] author proposed a mechanism to secure the communication in WBANs. This mechanism is based on biometrics method in which an intrinsic characteristics of patient body are utilized. The mechanism has authentication identity or secure distribution of cipher key to secure the data in WBANs. This mechanism is developed on symmetric cryptosystem to secure the m-health and telemedicine data. The author tested this system by collecting the previous data from two experiments electrocardiogram (ECG) and photoplethysmogram (PPG). Then, set the time synchronization process on different sensor nodes. This mechanism needs synchronization circuit to interact with the physiological signal detection to record the timestamp signal. However, this mechanism is only used for few applications and complex in nature.

Another biometric method to secure the wireless biosensors proposed by [x]. This method also known as automatic identification and verification of patient by their behavioral and physiological characteristics. This approach is for secure the WBANs data typically sent from external sensors. The biosensors are implanted or wearable sensors used to gather real time data from different parts of human body. Biometric approach utilizes to overcome the insecurity of WBANs sensors. This scheme secure the data by key distribution method without key exchange.

B. Secure Cross-layer Protocol

A Secure Cross-layer Protocol (CICADA-S) was [xv] proposed for WBANs. This protocol is enhanced version of CICADA protocol which is based on MAC and Network layer. The main aim of this CICADA-S is integrating the key management and provides security and privacy with low energy consumption mechanism. This protocol was a first protocol to address the life cycle of sensor nodes. The most important device in WBANs system is server which managed by medical center and hospital. In this protocol, author assumed that server is physically protected. In this protocol, in start of every data transfer cycle' the slots are assigned and every parent node send a SCHEME-message to all children nodes. In addition, every cycle is divided into two parts: control and data sub cycle. Whenever, all node received their scheme, the control sub-cycle is ended and data sub-cycle started. This protocol has simple mechanism and implemented on any devices with low cost hardware changes. However, the WBANs systems are more complicated and dynamic in nature. This type of simple schemes have some limitations especially for inter body sensor nodes where human body position is not static.

C. Integrated Biometric-based Security Framework

An Integrated Biometric-based Security Framework [xvi] was proposed based on Wavelet-Domain Hidden Markow Model (HMM) for WBANs. This security framework is based on biometric features shared by body sensors. The data communication among sensor nodes are secured via this encryption scheme. This scheme requires low computational power, less bandwidth and energy. The scheme utilized a wavelet-domain Hidden Markow Model (HMM) for accurate authentication and non-Gaussian statistics of electrocardiogram signals. Biometric information is based on human different features such as fingerprint, iris and handwriting. This scheme integrated biomedical information including processing power, sensing and transmission. For classification, the HMM

as a statistical model is utilized as a flexible and adaptability tool. However, this scheme is still suffered with unaffordable mechanism due to communication overhead and power inefficiency. The existing schemes neglect patient mobility, computational power inefficiencies and sensor energy. Fig. 2, shows the integrated system and its main components.

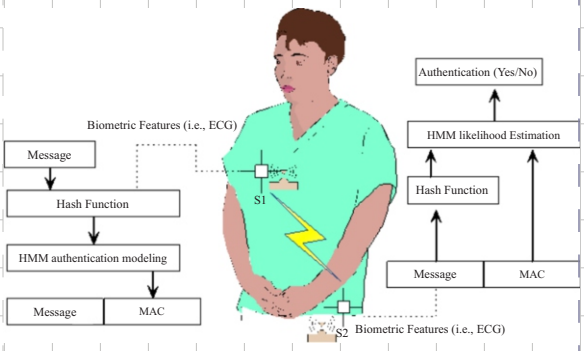

Fig. 2. Integrated Biometric-based Security System

D. *Secure Ad-hoc Trust Initialization and Key Management Protocol*

In [xvii] authors proposed a Group Device Pairing (GDP) based on multi-party authentication key management protocol. In this protocol, a group of sensor nodes in WBANs established initial trust by generating various shared secret keys out on unauthenticated channel. The working cycle of WBANs has three main phases including pre-deployment, deployment and working phases. In first phase, the sensor nodes are establishing initial shared secret by PDP. After running the PDP, every sensor nodes derives an individual symmetric secret key with the controller. Then, the group key and pairwise key is established. Afterwards, the Group Device Pairing (GDP) is used to for multi-party authentication. In deployment phase, the sensor nodes are deployed around the human body and pairwise keys are computed, and logical key is established. However, due to different protocols this proposed work has some computation complexities which leads to network overhead.

E. *Biometric-based Security for Data Authentication*

In [xviii] authors proposed a Biometric-based Security for Data Authentication in WBANs. They proposed model based on communication medium data authentication security with less computational complexity and power efficiency. The model adopted biometric characteristics to secure the data communication by an authentication process. Biometric refers to an automatic verification or identification of individual behavioral and physiological characteristics. In WBANs, biometric approach is used an intrinsic features of patient body as an authentication identity in order to secure the distribution of cipher key for WBANs communication. Author selected a sender electrocardiogram feature as a biometric key for data authentication method. The patient record sensed and cannot mixed with other records. This model utilizes one type of feature as a biometric key. However, the health care applications are based on different purposes and variety of applications are working on one patient. This type of model is limited in nature and based on one feature which is not suitable for recent WBANs applications.

This section presented the state of the art security protocols available for WBANs. To conclude this section, a summery and comparison of the existing security protocols is presented in Table I.

TABLE I
COMPARISON OF EXISTING SECURITY PROTOCOLS IN WBAN

Protocols	Issues Addressed	Adopted Approach
Secure Mechanism [xiv]	Eavesdropping, injection, and modification of packets	Biometrics method
Biometric secure method [xiv]	Eavesdropping, identity spoofing, or redirection of the data to non-legitimate users	Biometrics method, Keys distribution
CICADA-S [xv]	Malicious node	Key management and secure privacy preserving communication techniques
GDP [xvii]	Eavesdropping, injection, and modification of packets	Multi-party authenticated key agreement
Biometric-based Security Data Authentication [xviii]	Eavesdropping, injection, and modification of packets	Biometrics method, encryption
HMM [xvi]	Unsecure virtual channels data transmissions	Biometrics method, wavelet-domain statistic approach
Elliptic Curve Cryptography (ECC) [xix]	Replay attack, unsecure data communication	Elliptic Curve Cryptography

IV. PROPOSED METHOD FOR DATA SECURITY IN WBANS

The proposed method (D-Sign) is based on hybrid approach by using secret keys and digital signatures for securing data in WBANs. This method is more secure because of its randomness property for secret keys for data encryption and decryption. It provides better

security for protecting sensory data in WBANs.

The proposed method uses secret keys which are shared with the BNC and all the sensor nodes in the network. Each sensor node get registered with the BNC so that BNC can save the basic information of the sensor nodes in the network. Then, the BNC randomly picks a pairwise key from the key-pool and assigns to that node to establish the trust relationship with it. The public keys (PK) and secret keys (SK) are loaded in the system. The BNC signs each data packet with a SK by digital signatures and broadcasts the PK to all the sensors nodes in the network.

In this method, each data packet is validated by the BNC before further sending to the medical server. So if any bogus packets is found, it is discarded at this stage. The BNC also check the validity and freshness of SK. If found incorrect, the BNC immediately discard the SK and drop the trust relation with that sensor node. The BNC further request that sensor node to send alternate SK to establish trust and authenticate the data packets from that particular sensor node. On the other hand, if data packet is authenticated, the BNC endorsed the packet by using digital signatures and forward it to the medical server for further processing. On receiving the data packets, the medical server checks the digital signatures and freshness of data packets. The digital signatures ensure that the data packets are accurate and free from any fake information. The proposed D-Sign method works in the following steps:

i) Generating Hash Value

The proposed D-Sign method used SHA-1 hash function to encrypt original sensory data into a fixed size bits strings called hash values as shown in Fig. 3.

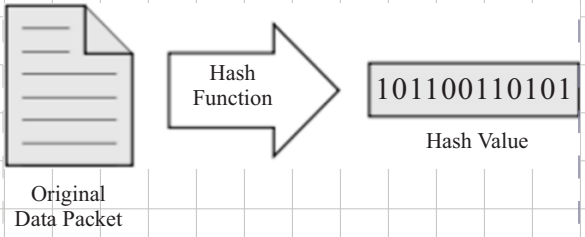

Fig. 3. Generating hash value

ii. Applying Digital Signatures

The hash value generated is then encrypted with senders PK. The hash value and the sender's SK are generates digital signature, which is added to the data packet (as shown in Fig. 4) before sending packet over the network.

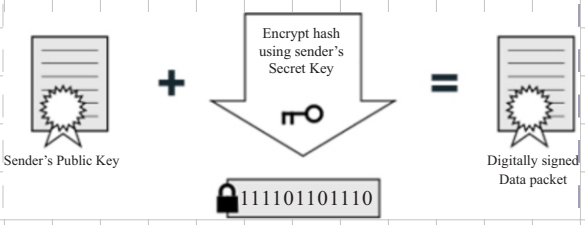

Fig. 4. Generating digital signatures

iii. Verifying the Digital Signatures

When BNC receive the packet, it uses the sender's PK (which is already added in the digital signature) to decrypt the hash value. The BNC computes a new hash value for the packet. If the new hash is same as that of decrypted one, the BNC identifies that the packet is not modified. Additionally, the BNC also ensures from its key tables that the PK attached in the digital signatures is really belongs to the same sending node. The Fig.5, shows the overall verification process of the digital signatures.

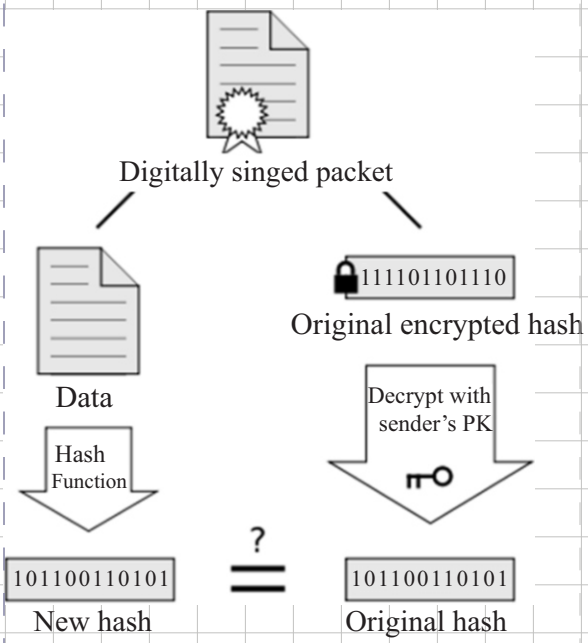

Fig. 5. Verification process of the digital signatures

V. Results and Discussions

This section presents the performance evaluation of the proposed method (D-Sign) for securing data communication in WBANs. The experimental results are compared with the state of the art methods available for the purpose of data security in WBANs.

Fig. 6 demonstrates the comparison of D-Sign, ECC and GDP protocols in terms of initial trust establishment. The results shows that the proposed D-Sign protocol took less time to establish trust relationship between BNC and sensor node. This is because of the simplicity of the hybrid approach used for securing data communication in WBANs.

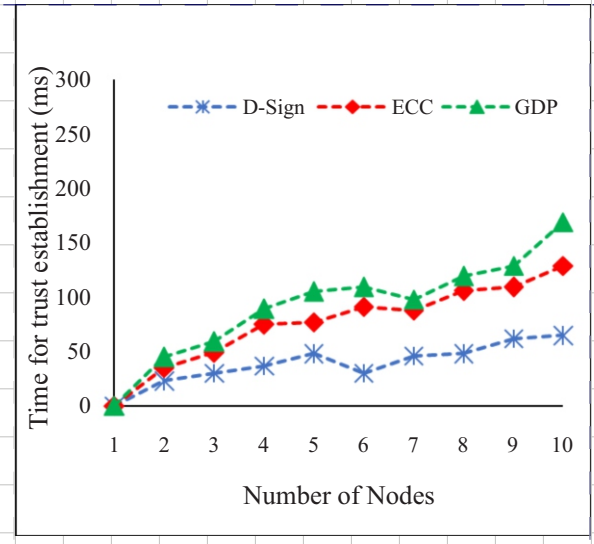

Fig. 6. Time required for initial trust key establishment

The Fig. 7, show the comparison of authenticity and accuracy of data received at the destination i-e medical server. The results shows that the proposed D-Sign protocol outperforms comparing to the ECC and GDP protocols. This is because of dual authentication approach is used in proposed method i-e data encryption and digital signatures.

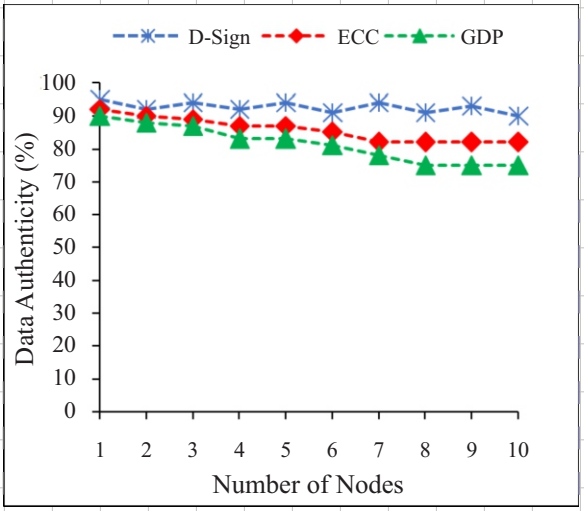

Fig. 7. Analysis of accuracy of data received at medical server

The Fig. 8, show the comparison of end-to-end delay for packet sending. The results depicts less end-to-end delay by proposed DSign protocol comparing to the ECC and GDP protocols.

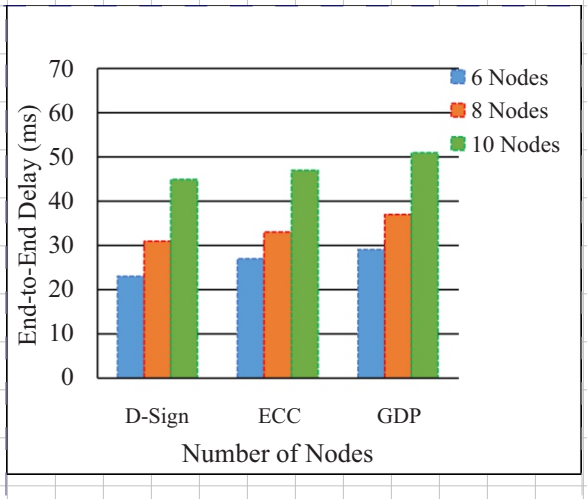

Fig. 8. Comparison of end-to-end delay

VI. Conclusion

The privacy and security of patient data is an important area of research. The WBANs data communication is mostly based on wireless communication and may lead to various different security threats and attacks. If the patient information is compromised it may leads to serious issues for patient health. Security issues in WBANs networks are categorized into two broad level that are system and information security. The attackers steal patient information by eavesdropping the wireless communication. There are many security threats in WBANs such as data modification, impersonation, replaying. In order to address these security threats, various security schemes have been proposed based on data integrality, authentication, encryption and freshness protection. However, these encryption schemes have complex mechanism and cause of communication overhead and power inefficiency. The proposed method uses hybrid method by using digital signature along with encryption and decryption technique. The results show that the proposed method is more efficient in terms of securing data and using optimal resources in the network.

References

[i] C. Zhu, C. Zheng, L. Shu, and G. Han, "A survey on coverage and connectivity issues in wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 35, no. 2, pp. 619–632, 2012.

[ii] N. A. Pantazis, S. A. Nikolidakis, and D. D. Vergados, "Energy-Efficient Routing Protocols in Wireless Sensor Networks: A Survey," *IEEE Commun. Surv. Tutorials*, vol. 15, no. 2, pp. 551–591, 2013.

[iii] I. F. Akyildiz, W. Su, Y. Sankara subramaniam, and E. Cayirci, "Wireless sensor networks: a

survey," *Comput. Networks*, vol. 38, no. 4, pp. 393–422, 2002.

[iv] B. Latré, B. Braem, I. Moerman, C. Blondia, and P. Demeester, "A survey on wireless body area networks," *Wirel. Networks*, vol. 17, no. 1, pp. 1–18, 2011.

[v] R. Cavallari, F. Martelli, R. Rosini, C. Buratti, and R. Verdone, "A Survey on Wireless Body Area Networks: Technologies and Design Challenges," *IEEE Commun. Surv. Tutorials*, vol. PP, no. 99, pp. 1–23, 2014.

[vi] M. Anwar, A. H. Abdullah, K. N. Qureshi, and A. H. Majid, "Wireless Body Area Networks for Healthcare Applications : An Overview," *TELKOMNIKA*, vol. 15, no. 3, pp. 1088–1095, 2017.

[vii] A. Sangwan and P. P. Bhattacharya, "Wireless Body Sensor Networks: A Review," *Int. J. Hybrid Inf. Technol.*, vol. 8, no. 9, pp. 105–120, 2015.

[viii] D. D. Van, Q. Ai, and Q. Liu, "Vertical handover algorithm for WBANs in ubiquitous healthcare with quality of service guarantees," *Inf.*, vol. 8, no. 1, 2017.

[ix] S. Ullah, M. Mohaisen, and M. A. Alnuem, "and Security Specifications," vol. 2013, 2013.

[x] M. K. Shahzad and T. H. Cho, "Extending the network lifetime by pre-deterministic key distribution in CCEF in wireless sensor networks," *Wirel. Networks*, vol. 21, no. 8, pp. 2799–2809, 2015.

[xi] R. Kumar, "State Of The Art : Security In Wireless Body Area Networks," *Int. J. Comput. Sci. Eng. Technol.*, vol. 4, no. 5, pp. 622–630, 2013.

[xii] I. A. Al-rassan and N. Khan, "Secure & Energy Efficient key Management Scheme for WBAN – A Hybrid Approach," vol. 11, no. 6, pp. 169–172, 2011.

[xiii] M. Li, W. Lou, and K. Ren, "Data Secutiry and Privacy in Wireless Body Area Networks," *IEEE Wirel. Commun.*, vol. 17, no. 1, pp. 51–58, 2010.

[xiv] P. Abina, K. Dhivyakala, L. Suganya, and S. M. Praveena, "Biometric Authentication System for Body Area Network," *Int. J. Adv. Res. Electr.*, vol. 3, no. 3, pp. 7954–7964, 2014.

[xv] D. Singel, "A Secure Cross-Layer Protocol for Multi-hop Wireless Body Area Networks," *Network*, pp. 94–107.

[xvi] H. Wang, H. Fang, L. Xing, and M. Chen, "An integrated biometric-based security framework using wavelet-domain HMM in wireless body area networks (WBAN)," *IEEE Int. Conf. Commun.*, 2011.

[xvii] M. Li, S. Yu, J. D. Guttman, W. Lou, and K. Ren, "Secure ad hoc trust initialization and key management in wireless body area networks," *ACM Trans. Sens. Networks*, vol. 9, no. 2, pp. 1–35, 2013.

[xviii] S. N. Ramli, R. Ahmad, M. F. Abdollah, and E. Dutkiewicz, "A Biometric-based Security for Data Authentication in Wireless Body Area Network (WBAN)," *Adv. Commun. Technol. (ICACT), 2013 15th Int. Conf.*, no. January, pp. 998–1001, 2013.

[xix] Y.-S. Lee, "Secure key management scheme based on ECC algorithm for patient's medical information in healthcare system," *Int. Conf. Inf. Netw. 2014*, no. February, pp. 453–457, 2014.