Scope International Journal of Science, Humanities, Management and Technology. ISSN : 2455-068X

Vol.3 Issue 4 (2017) 132 - 136. Submitted 25/11/2017. Published 30/12/2017

EFFICIENT CERTIFICATELESS ACCESS CONTROL FOR WIRELESS BODY AREA NETWORKS

[1]S. Bakyalakshmi, M.Phil Scholar, Department of Computer Science, Bharathiyar Arts and Science college for Women, Deviyakurichi, Thalaivasal, Salem.

[2]C. Renuga, Assistant Professor, Department of Computer Science, Bharathiyar Arts and Science college for Women, Deviyakurichi, Thalaivasal, Salem.

Abstract:

Low computational power of wireless sensors and the multicast form of transmission exhibited by WBAN make it susceptible to several security and privacy issues. Due to these, many security and privacy preservation approaches had been proposed to secure and preserve privacy of wearable WBAN systems. However, the inherent low computational power which characterises WBAN nodes made most of these approaches inefficient for the networks. This paper proposes a lightweight two-way but coordinated perturbation scheme for obfuscating both the identities and measurements of the sensor in the wearable WBAN system. The coordinated generation of perturbs eliminates security and privacy problems associated with reconstruction by the receiver. The results showed that the scheme outperforms these schemes in terms of computational overhead. The scheme was also evaluated by simulating the scheme using digital ECG sensors as WBAN nodes. The simulation results not only confirm the estimated speed but also showed that the scheme left no semantic pattern in the transmitted data.

Keywords: WBAN, ECG, Transmitted.

1. INTRODUCTION

Acquisition of accurate health knowledge of hu- man anatomy and condition is the major operation that helps health-care professionals or doctors in handling health related issues of their patients. Most of the major health complications can easily be averted if useful information are readily available for health-cares professionals. The wireless body area network has emerged as a new technology for healthcare delivery. It monitors and commu- nicates patients vital body parameters and move- ments through small wearable or implantable sen- sors over short-range wireless communication. Al- though, WBAN easily solves the problem of timing Acquisition of accurate health knowledge of hu- man anatomy and condition is the major operation that helps health-care professionals or doctors in handling health related issues of their patients. Most of the major health complications can easily be averted if useful information are readily available for health-cares professionals. The wireless body area network has emerged as a new technology for healthcare delivery. It monitors and communicates patients vital body parameters and movements through small wearable or implantable senors over short-range wirelescommunication. Al- though, WBAN easily solves the problem of timingand non-availability of patients health information in health-care system, however wireless communication is not secured. This subjects health information to different forms of attacks. Preservation of identity and securing data transfer from the user to the server or sensors data stored in the server are the major challenges of WBAN. Examples of these se- curity challenges are snooping, routing attacks and spoofing which affect the data confidentiality, data integrity, data availability and privacy of the sensor node. Several schemes had been proposed to secure health information in resources

constraint WBAN. However, most of these schemes are either network specific or based on public or private key infrastruc- ture which requires considerable memory and com putational resources. These make them unsuitable for resources constraint network such as WBAN. In view of this, a lightweight but efficient security and privacy mechanism is required for WBANs routing protocol in order to protect sensitive data and wearer privacy during data transfer.

2. LITERATURE REVIEW

Wireless Body Area Network, as shown in Figure 1, is a set of sensor with wireless communication capabilities placed on human body for physiological monitoring of some of the body quantities to pre- vent complications and prompt diagnosis of health conditions. Sensor nodes are characterised with low power and computational capacity. Therefore, it must be subjected to low power and computational tasks in order to carry out its operation for a considerable period of time. The current develop- ments and future direction of research on wearable WBAN systems for continuous monitoring of out and in-patients are inherently showing the need to improve on the security and privacy of sensor. Also, there is considerable increase in the number of the security threats.

In, a scheme was proposed to secure cardiography information by using a lightweight en- cryption framework to augment compression during sampling by using the measurement matrix as a symmetric key for encryption and decryption. The symmetric key was extracted from Received Signal Strength Indicator (RSSI) values which was used as seed to feed a Linear Feedback Shift Register (LFSR) to generate an m-sequence. This would be reorganised to form CS sensing matrix by the receiver and transmitter. However, this method is sensor dependent, that is, it is built around ana- log sensors which output must be converted to binary data before transmission.

WSN topologies, data sharing mechanisms, cryptography and attributes-based encryption in privacy preserv- ing. In their work, some cryptography issues such as storage or computational overhead, the trade-off between the security and elasticity, trust assurance against the attacks were discussed. They made it clear that the secure data transfer from the user to the server is the major issue against the network ad-versaries. They highlighted the major cryptography operations such as key generation, encryption, and decryption as the main sources of storage and com- putational overheads and delegation issues in data preserving.

3. PROPOSED SYSTEM

In this work two problems were formulated in order to address the security and privacy issues in WBAN. These are how to secure data in resource-constraint WBAN, and an efficient 2-way coordinated perturbs generation technique to secure data and preserve the privacy of wearers in WBAN. Formulation of coordinated 2-way perturbation parameters. The major issue in data obfuscation using perturbation is how to generate perturbs such that each sensor's perturb can be re- generated only by the authorised receiver without compromising its knowledge to the adversary. That is, there must be a form of authentication and exchange feature(s) inherent in the perturb generation procedure otherwise reconstruction of data by receiver will not be possible. In most perturbation schemes, this coordination is a weak link through which adversary launches attacks. In this work, a set of cryptography operations which allow sensor to create root parameters for any authorised users to unperturb any of its perturbed measurements is used. privacy schemes developed for WBAN. In light of this, the propose scheme engages a few exponential operations for data and identity obfuscation. Data perturbation and transmission are done through the WBAN gateway

(sink). The WBAN is modelled such that registration and parameters exchange are between WBAN sink and authorise users. During registration, the sink and user obfuscatory exchange their session identities and time-stamp using the propose novel obfuscatory exchange method used in registration and 2-way coordinated perturb gen- eration phases.

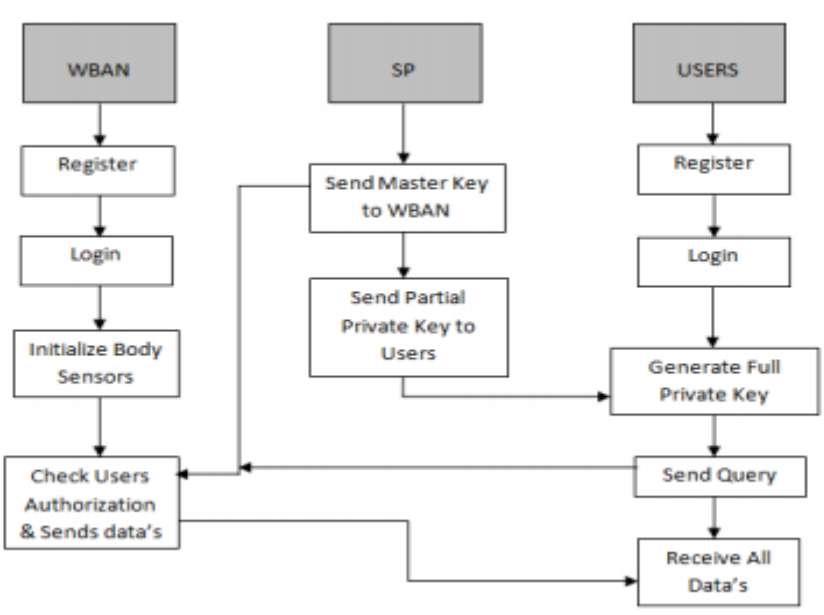

Fig.1.Proposed System

Then, sink initiates 2-way coordi- nated perturb generation by generating perturbation parameters Ps, blinds and sends it to the user. This procedure is repeated by user by generating its own perturbation parameter Pa, blinds and sends it to sink. Each of them unblind the received perturbation parameter to compute the session perturb Pt. The source node perturbs its message with Pt and sends it to the user for a real time use or stores it in cloud server for future use. Since user has Pt, it can reconstruct message from perturbed message anytime. Wireless Body Area Networks (WBAN) consists of aggregate number of sensor nodes and controller attached to the Base Station. The sensor node is embedded into the tissue of human body. The service provider helps to monitor the patient's health conditions. The data is collected and processed only from the authorized users. It acts gateway between user and WBAN servers. Once the user get enrol with the SP, then the user can access the data. The secret key is generated by the Service Providers. Henceforth, SP should be legal and ensures better data confidentiality and integrity services. In this step, we design an efficient certificateless access control scheme for public verifiability and ciphertext authenticity. Signcryption based access control model ensures least computational cost and less energy consumption by sensor nodes.

4. ANALYSIS

Wireless body area networks (BANs) have drawn much attention from research community and industry in recent years. Multimedia healthcare services provided by BANs can be available to anyone, anywhere, and anytime seamlessly. A critical issue in BANs is how to preserve the integrity and privacy of a person's medical data over wireless environments in a resource efficient manner. In this paper, we propose an enhanced certificateless signcryption scheme which authorizes the users and transmit the data to the

concerned users.Security is a significant metric that has to be focused over the outsourced e-health data. Most of the healthcare networks get attracted by the WBAN technologies. The transition over EHRs is a demanding issue with affordable costs. Thus, the deployment of cryptographic model is employed over the e-health records. Experimental analysis is processed for the predefined set of sensor nodes. Any users can access the data within stipulated period of time with security analysis in terms of efficient key generation, processing cost and energy consumption.

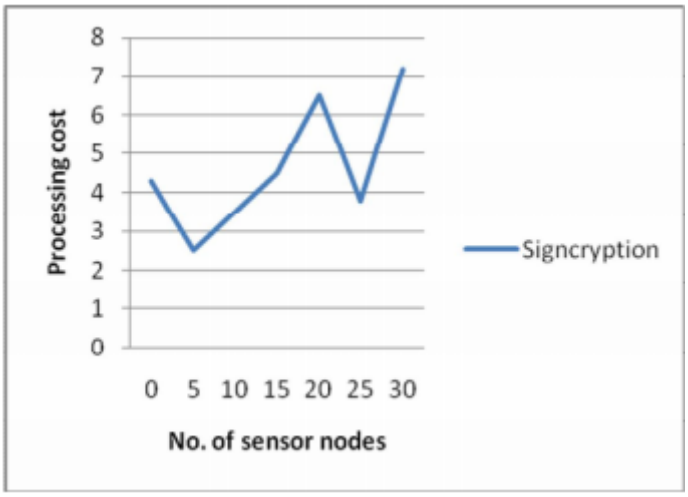

Fig.2.Wave output

The main purpose is to devise the access control model with the qualities of lessened storage space and rapid retrieval functionalities. This section presents the experimental analysis of our proposed certificateless signcryption scheme using WBAN networks and WBAN servers. The objective of the study is to effectively utilize the energy of the nodes with reduced data loss and without compromising the accuracy of authentication.

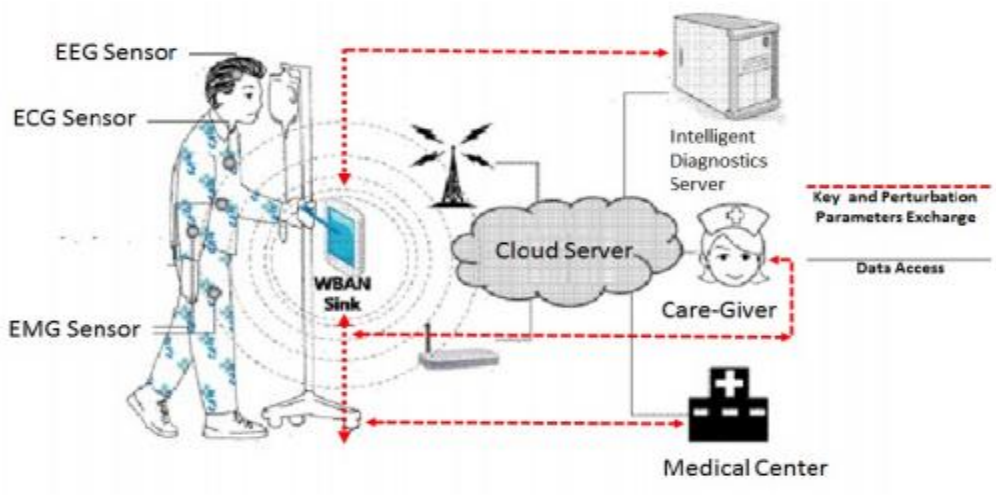

Fig.3.System Model

While doing the protocol analysis, the processing cost taken by tree are eliminated. Since, the certificateless signcryption scheme takes the security parameters with certain limitations which depicts less bits of key processing is used. Semantic insecurity of perturbed data is another threat considered. This form of insecurity on the perturbed data is usually caused by the semantic pattern which is inherent in the sensor data. For example, if the variation in the data sizes are wide some level of information could be gleaned by adversary despite being perturbed. Semantic issue is addressed in the scheme through the generation of large size perturb for perturbation of sensor data before being transmitted so as to completely mask off the uneven variation of the data set.

CONCLUSION

In this work, a lightweight scheme for securing data and preserving the privacy of wearer of WBAN in e-health is proposed. The scheme is resilient to malfunction associated with computation power, energy consumption and with no semantical pattern in the transmitted data. Compare to the other WBAN security schemes, the proposed scheme outperforms the other state of the art schemes in terms of computational overheads and capable of securing data with no semantic pattern.

REFERENCES

[1] V. Agrawal. ”Security and privacy issues in wireless sensor networks for healthcare”. In Internet of Things, User-Centric IoT, LNICST 150, Springer, Cham, pages 223-228, 2015.

[2] P. Gong, T. Chen, and Q. Xu. ”ETARP: An Energy Efficient Trust-Aware Routing Protocol for Wireless Sensor Networks”. Journal of Sensors, 2015(1), pages 1-10, 2014.

[3] C. Karlof, and D. Wagner. ”Secure routing in wireless sensor networks: attacks and countermeasures”. Journal of Ad Hoc Networks, 1(2003), pages 293-315, 2003.

[4] F. Huei-Wen, and D. Rachmarini. ”A secure routing protocol for wireless sensor networks with consideration of energy effi- ciency”. In IEEE Network Operations and Management Sympo- sium (NOMS), pages 105-112, 2012.

[5] D. Ruslan and R. Gill. ”Securing While Sampling in Wireless Body Area Networks With Application to Electrocardiography”. IEEE Journal of Biomedical and Health Informatics, 20(1), pages 1-7, 2016.

[6] A. Matthew, and S. Thomas. ”General Deviants: An Analysis of Perturbations in Compressed Sensing”. IEEE Journal of Selected Topics in Signal Processing, 4(2), pages 342-349, 2010.