International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 5
May 2017

# Authentication using LDAP in Wireless Body Area Network

**Miss W. S. Dharme.**
SGBAU, Amravati
India.

**Dr.R.V.Dharaskar.**
Director, MPGI, Nanded
India.

**Dr.V.M.Thakare.**
SGBAU, Amravati
India.

## ABSTRACT

*Wireless body area network was proposed in 1996. Wirelessbody area network is one of the wireless sensor technologies for improving healthcare service.Wirelessbodyarea network has been improving in healthcare qualitynot only forpatients but also for medical staff. This paper focuses on given below techniques i.e, electrocardiogram (ECG) based BS generation method, anonymous authentication(AA) scheme, certificateless signature (CLS) scheme, A pair of lightweight and efficient authentication protocols is used for enable the remote WBAN users for enjoying healthcare services in the CLS scheme. In anonymous authentication AA scheme, it is useful for providing security by protecting the patient's identity and encrypting medical data. To improve the time efficiency, this paper focused on an ECG Multiple Fiducial-points based Binary Sequence Generation (MFBSG) algorithm. This MFBSG method can generate five feature values from one heart beat cycle and it is up to five times faster than the solely IPI-based method. The proposed method achieves satisfactory results.*

**Index Terms**—***Authentication, wireless body area network, security, wavelet transform,healthcare, Attack.***

## I) INTRODUCTION

The wireless body area network (WBAN),is a promising networking paradigm, whichuses wireless personal area network (WPAN) technology. Inrecent years, the WBAN has attracted a lot of attention fromboth the research community and industry as an important partof the Internet of Things (IoT).WBANsnot only bring us conveniences but also bring along the challengeof keeping data's confidentiality and preserving patients'privacy. In the past few years, several anonymous authentication(AA) schemes for WBANs wereproposed to enhance security byprotecting patients' identities and by encrypting medical data.The electrocardiogram (ECG) based data encryption EDE is designed with the ability to provide information-theoretically unbreakable encryption where two well-known techniques of error correcting codes and classic one-time pads (OTPs) are combined to achieve a cryptographic primitive for IMDs [1]. The rapid increase in healthcare demand has seen novel developments in health monitoring technologies, such as the body area networks (BAN) paradigm[2].A Survey on Intrabody Communications for Body Area Network Applications. Here author discussed Intrabody communication (IBC) is a new data transmission concept that uses human body as a communication channel to transmit data [3]. Data Authentication Model achieves security at the expense of less usage of resources and lower computational power [4].

This paper, discusses the methods, i.e. electrocardiogram (ECG) based BS generation method, anonymous authentication (AA) scheme, certificateless signature (CLS) scheme. The idea behind this paper is to improve security levels in Wireless Body Area Network.

## II) BACKGROUND

By processing the Inter-pulse Intervals (IPIs) of ECG signals ECG-based BSes are randomly generated. ECG based mechanism generate binary sequences from ECG signals [1]. To obtain the feature values from one heart beat cycle the proposed MFBSG algorithm uses the multiple fiducial points. The MFBSG algorithm uses discrete wavelet transform to detect fiducial points and to process ECG signals. MFBSG algorithm exploits multiple ECG feature values, including PR, RQ, RS, RP and RT intervals that randomly generates BSeswith low latency.

For Wireless body area network, AA schemes is secure but by demonstrating it is not secure against impersonation attack and for applications based on WBANs. While satisfying security requirements in WBANs a security analysis shows that the AA scheme is secure. Compared to

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 5
May 2017

Liu.et al.'s scheme AA scheme has the same computation cost. For practical WBAN application scenario AA scheme is more suitable [2].

The low-power wireless sensor nodes are used to gather biomedical information for various applications such as residential, hospitals and work environments in WBAN [3].

The Data Authentication Model achieves authenticity and confidentiality with the help of private key prior to the message transfer that is distributed among both parties. It achieves security at the expense of less usage of resources and lower computational power[4].

This paper introduces authentication scheme in WBANs as**Section I** Introduction. **Section II** discusses Background. **Section III** discusses previous work. **Section IV** discusses existing methodologies. **Section V**discusses analysis of proposed method. **Section VI** proposed method and outcome result possible. Finally **section VII** Conclude this review paper. Lastly, **section IX** gives the future scope.

## III) PREVIOUS WORK DONE

G. Zheng et al. (2015) [1] proposed the method Encryption for implantable medical devices using modified one-time pads. The electrocardiogram (ECG) based data encryption EDE is designed with the ability to provide information-theoretically unbreakable encryption where two well-known techniques of error correcting codes and classic one-time pads (OTPs) are combined to achieve a cryptographic primitive for IMDs.The EDE design achieves a balance of a high accessibility and high security for the IMD. The EDE scheme includes two components: an external programmer and an IMD. The IMD is an electronic device whichis implanted to assist health of patient and the programmer is an outside device which has the ability to program wirelessly and to access data in the IMD.

M. Samaneh et al. (2014) [2]have proposed Wireless body area networks: A survey, here the author discussed the rapid increase in healthcare demand has seen novel developments in health monitoring technologies, such as the body area networks (BAN) paradigm. BAN technology envisions a network of continuously operating sensors, which measure critical physical and physiological parameters e.g., mobility, heart rate, and glucose levels.

M. Seyedist al. (2013) [3] has proposed A Survey on Intrabody Communications for Body Area Network Applications. Here author discussedIntrabody communication (IBC) is a new data transmission concept that uses human body as a communication channel to transmit data. One of the main objectives of research into intrabody communication is the characterization of the human body as a transmission medium for electrical signals.

S. Sridharan et al. (2013) [4] has proposed Secure Data Authentication Model for Online Health Monitoring System here author discussed a secure data authentication model for the wireless body area network using a single private key exchanged during the time of configuration. The need for secure data exchange grows rapidly due the fact that the data exchanged are confined to the details of the ailing patient.

## IV) EXISTING METHODOLOGIES

### A. ECG based BS generation method:

Many authentication methods for Wireless Body Area Network have been implemented over the last several decades. There are different methodologies that are implemented for authentication in Wireless Body Area Network. Binary Sequence (BS) is a sequence of bit values of 0 & 1 and sequence of N bits. To improve the time efficiency an ECG Multiple Fiducial-points based Binary Sequence Generation MFBSG algorithm is used. The BS generation method removes sampling noise and samples ECG signals. It runs through following two processes:

1) ECG Wavelet Process:

This Wavelet Transform (WT) technique can represent features of ECG signals at different resolutions. WT uses a series of small wavelet. For a wavelet function ω (t), the wavelet transform of a signal f (t) € $L^2$(R) is given by

$$W_{f(a,b)} = \frac{1}{\sqrt{|a|}} \int_{-\omega}^{\omega} f(t)\ ^{\varphi} * \left(\frac{t-b}{a}\right) dt$$

Where a is scale factor, b is translation of ω(t).

2) BS Generation Process:

BS generation process uses five types of features from each ECG heartbeat cycle. The purpose of this

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 5
May 2017

process is to generate random BSes Inter-pulse Intervals (IPIs) of ECG signals [1].

**B. Anonymous Authentication (AA) scheme:**

The Anonymous Authentication scheme consists of the three algorithms: Initialization, Authentication and Registration. The AA scheme has some security requirements such as Mutual Authentication, Session Key Agreement, Non-traceability, Anonymity and so on. The AA scheme is provably secure for Wireless Body Area Network [2].

**C. Certificateless Signature (CLS) Scheme:**

The CLS scheme is based on bilinear pairing. The CLS scheme is efficient, cost-effective, secure against existential forgery on adaptively chosen message attack in the random oracle model. The certificateless signature scheme has a potential to achieve more desirable security properties with less computational cost [3].

**D. Data Authentication Model:**

All the transactions in the Data Authentication Model happen only after the recognition process. The phases in the Data Authentication Model are: Private Key Establishment and Medical data Transfer. The private key is established for the configuration process for the entire health monitoring system. The Medical Data Transfer is the patient's medical data transfer with security, authenticity and accuracy being the main concern at highest level in receiver end [4].

## V) ANALYSIS AND DISCUSSION

An authentication protocol has the characteristics of public key replacement attack resistance as well as high computational efficiency. The security features comparison between the scheme and other protocols shows that the scheme can provide security guarantee to WBAN. The protocol reaches anonymity, mutual authentication, non-reputation and some other security features.Unlike other ECG-based key agreement schemes where ECG features are used in the EDE scheme, to facilitate a key distribution, and random binary strings generated from ECG signals are directly used as keys for encryption [1].

Wireless connectivity in BAN technology is a key to its success as it grants portability and flexibility to the user.A security analysis of AA scheme shows that the scheme is provably secure. A performance analysis shows that AA scheme is more suitable for practical WBAN scenarios. To enhance security the AA scheme is effective in wireless body area network system [2].

The proposed CLS scheme is designed for two remote anonymous authentication protocols, which are particularly suitable for resource-constrained mobile clients. To access WBAN services, the protocols use an anonymous account index instead of a WBAN client's real identity, thereby preventing the potential privacy leakage to network manager (NMs) and application providers (APs)[3].

Data Authentication Model achieves higher levels of authenticity, confidentiality, security at expense of less usage of resources and lower computational power. In data authentication model low cost authentication challenges areaddressed. Instead of complex cryptographic key distribution algorithm a simple shared private key technique is used [4].

| Authentication Techniques | Advantages | Disadvantages |
|---|---|---|
| ECG based BS generation method | Achieves low-latency. | High timing efficiency |
| Anonymous authentication scheme | 1) AA scheme is provably secure while satisfying security requirement in WBANs.<br>2)AA scheme is more suitable for practical WBAN application scenario. | The scheme cannot withstand the impersonation attack. |
| Certificateless signature scheme | A potential to achieve more desirable security properties with less computational cost. | Obtains higher efficiency. |
| Data Authentication Model | Achieve confidentiality and authenticity. | Computational complexity |

**TABLE 6: Comparisons between different techniques for Wireless Body Area Network.**

## VI) PROPOSED METHODOLOGY

In this paper Lightweight Directory Access Protocol (LDAP) directories and LDAP authentication have become one of the enterprise user infrastructure cornerstones. In most medium to

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 5
May 2017

large enterprises, the authoritative source for employee information is usually the Human Resource Management System (HRMS). Figuring out what system is authoritative for customers, contractors, temps, business partners and vendors is usually much more complicated. It is very important before LDAP authentication is implemented the enterprise first determines which system or application will be authoritative for the identity data. This also means cleaning up the associated business processes dealing with identity creation, role changes and terminations. Often the authoritative identity source will have many identities in their data stores listed as active who are no longer active. This can create security holes in any LDAP authentication.LDAP authentication relies upon the LDAP directory having the most up to date identity information with which to do an authentication against. This requires that the authoritative source be linked, at a minimum, on a nightly batch basis, and in many cases, on a identity event basis.

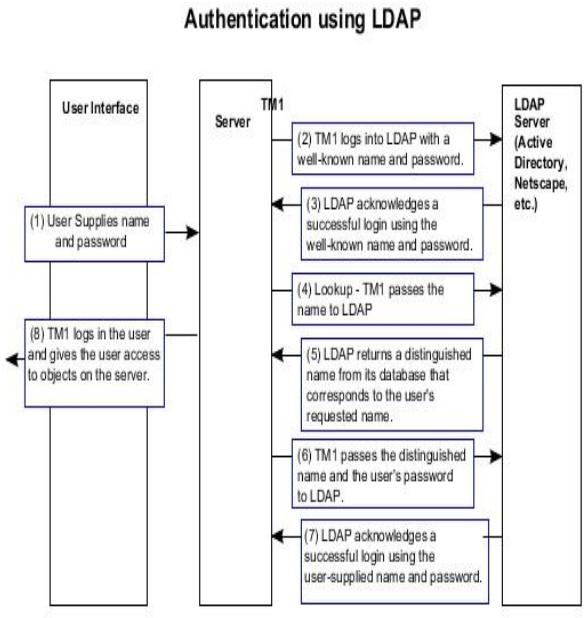


**Figure. Authentication using LDAP**

In the old days, of a few years ago, interfacing LDAP directories with authoritative source data bases was expensive and time consuming to do. The synchronization of the LDAP directories with the databases was critical and costly. Today however, LDAP virtual directories are now mainstream tools. A LDAP virtual directory is one which sits in a virtual environment and has its sources of identity information derived from pointers to specific tables in data stores or, in other LDAP directories.

The user usually enters in their id and password. The information may be presented as an online form or simply have an entry point for the id and password. This information is then sent to the LDAP directory (make sure the information is sent encrypted and not in open text).The directory takes this information and compares it to the id and password stored in the LDAP directory. If it is the same, the LDAP authentication is successful. In network operating systems, the network then takes over and proceeds with user authorization and allows them to use the network.

## VII) POSSIBLE OUTCOME AND RESULT

LDAP authentication is now very common in network operating systems. They are very quick for doing identity reads against as compared to traditional databases. They are low cost - in fact some LDAP directories are available for free

Virtual LDAP directories enable quick linkage between multiple databases and multiple LDAP directories. LDAP directories are excellent for doing rapid LDAP authentication against for any digitized authentication.

## VIII) CONCLUSION

In this paper presents LDAP directory having the most up to date identity information with which to do an authentication against. LDAP directories are excellent for doing rapid LDAP authentication against for any digitized authentication. LDAP directories have a universal protocol enabling quick interaction and exchange of identity information between enterprises. The main objective of this paper is improving performance and reducing network load using LDAP directories that can be easily partitioned to place the directory close to the end user.

## IX) FUTURE SCOPE

In future, the proposed method can improving the performance and reducing network load using LDAP directories that can be easily partitioned to place the directory close to the end user. LDAP

directories are available for free Virtual LDAP directories enable quick linkage between multiple databases and multiple LDAP directories.

## REFERENCES

[1] G. Zheng, G.Fang, R. Shankaran, and M.orgun, "Encryption for implantable medical devices using modified one-time pads," *Access IEEE, vol. 3, pp.* 825-836, 2015.

[2] M. Samaneh, A. Mehran, L. Justin, S. David, and J. Abbass, "Wireless body area networks: A survey," *IEEE Commun. Surv., Tuts., vol. 16, no.3, pp. 1658-1686, Aug.19, 2014.*

[3] M. Seyedi, B. Kibret, D.T.H. Lai, and M. Faulkner, "A Survey on Intrabody Communications for Body Area Network Applications," *IEEE Trans. Biomedical Eng., vol*.60, no. 8, pp. 2067-2079, Aug. 2013.

[4] S. Sridharan and Gorthy Ravi Kiran, "Secure Data Authentication Model for Online Health Monitoring System," presented at the *Fourth International Conference on Computing, Communication and Networking Technologies (ICCCNT'13)*, June 2013.