European Journal of Molecular & Clinical Medicine
ISSN 2515-8260 Volume 7, Issue 4, 2020

An Efficient Authentication Scheme for IoT based WBANs

[1]S.Jaganathan, [2]M.A. Raja, [3]C.Santha Kumar, [4]S.Velmurugan

[1]Professor, Department of Electrical and Electronics Engineering, Dr.N.G.P Institute of Technology, Coimbatore, Tamil Nadu 641 048, jaganathangct@gmail.com
[2]Professor, Department of Electronics and Communication Engineering, Nehru Institute of Engineering and Technology, Coimbatore, Tamil Nadu 641 105, professormaraja@gmail.com
[3]Associate Professor, Department of Electrical and Electronics Engineering, K S R Institute for Engineering and Technology, Tiruchengode, Tamil Nadu 637 215, sss.santha79@ksriet.ac.in
[4]Associate Professor, Department of Electrical and Electronics Engineering, K S R Institute for Engineering and Technology, Tiruchengode, Tamil Nadu 637 215, velmuruganmec@ksriet.ac.in

Abstract— Due to the quick headway of remote advancements, remote body region systems (WBANs) have gotten broad consideration from the general population as of late. IoT-based WBANs are intended to give life support significantly by observing the essential body boundaries and the general situations of human bodies. These sensors gather the constant natural data, for example, circulatory strain, pulse and beat of a patient and afterward send the data through cell phones, for example, an information sink to a distant clinical worker. In light of the got data, the specialists and other clinical specialists can give appropriate diagnostics to the patients. They are utilized to give appropriate and opportune clinical diagnostics and invited method for electronic social insurance frameworks.

Keywords—body-parameters, e-healthcare systems, mobile device, remote medical server, wearable sensors.

1. INTRODUCTION

A body zone systems (BAN), moreover implied as a remote body zone systems (WBAN) or a body sensor systems (BSN) or a clinical body territory systems (MBAN), is a distant arrangement of wearable enrolling devices. Boycott devices may be embedded inside the body, embeds, may be surface-mounted on the body in a fixed position Wearable turn of events or might be went with contraptions which people can pass on in various conditions, in garments pockets, by hand or in different packs.

A WBAN system can use WPAN distant advances as entries to show up at longer ranges. Through entryway devices, it is possible to relate the wearable contraptions on the human body to the web. In this way, supportive pros can get to understanding information electronic using the web self-sufficient of the patient territory.

A WBAN offers new applications in the region of far off medicinal services watching, home/human administrations, sedate, blended media, sports and various other, all of which make piece of space of the unconstrained chance of improvement a WBAN offers. In the restorative field, for example, a patient can be equipped with a far off body zone compose involving sensors that persistently measure unequivocal regular limits, for instance, temperature, circulatory strain, beat, electrocardiogram (ECG), breath, etc.

WBAN system require certain safety efforts to ensure security, protection, information uprightness and secrecy of a patient's wellbeing records at all the occasions. A supporting WBAN framework must execute explicit security activities that assurance these highlights. Security and protection of patient data are the two vital highlights for inside each WBAN framework.

Security refers information is shielded from unapproved clients when being moved, gathered, prepared and remains securely put away. Then again, protection proposes the power to control the social affair and

use of one's close to home data. For example, a patient may require his details to not be shared among insurance agencies who could utilize this data to control his/her from the inclusion. All the more explicitly, strategic information inside a WBAN framework is amazingly touchy, that whenever spilled to unapproved faculty could prompt a few ramifications for the patient, for example, losing the activity, open embarrassment and mental flimsiness.

2. RELATED WORK

In this segment, we abridge the most significant existing exploration along three lines: (1) verifying individual (implantable) gadgets inside a BAN; (2) verifying the interchanges inside a BAN; and (3) character based cryptography for BANs. As far as we could possibly know, no earlier work examined the security of interchanges between a BAN and its outer clients aside from [1] with concentrating on verifying the correspondences (information encryption, get to control, and computerized signature) between the information controller and an outside client by means of fluffy trait based encryption and tending to self-ensuring electronic restorative records (EMRs) on cell phones and offline correspondences utilizing characteristic based encryption.

Security issues in the WBANs must be unwound before authentic improvement. Some ensured designs for the WBANs have been proposed for different security goals [2]. In 2013, Hu et al. examined how to verify the correspondence between external customers and the WBANs. Their answer is attribute based encryption (ABE) . In any case, the ABE may not be a fair choice since it requires some costly cryptographic exercises. These extravagant assignments are an overwhelming weight for asset limited sensor hubs. Lu et al.proposed a protection saving astute methodology for the WBANs. This method can get strong data strategy and transmission with unimportant security exposure. Zhao et al. analyzed the key organization issue of the WBANs. In order to diminish the imperativeness use, they used essentialness based multihop-course decision procedure and biometrics synchronization segment.

Since the wellbeing information put away in the WBANs assume a significant job in the therapeutic finding and treatment, we ought to unravel the security issues in the WBANs before authentic improvement. Starting late, some protected designs for the WBANs have been proposed from different sides. In 2013, Hu et al.talked about how to give a security instrument to the extra body correspondence. Their answer is to utilize the quality based encryption (ABE) . In any case, the ABE may not be a conventional choice in light of the fact that the exorbitant cryptographic activity is a substantial weight for asset constrained sensor hubs. Lu et al.gave a protection saving shrewd system for the WBANs. Zhao et al.talked about the key administration issue in the WBANs. In 2014, He et al. examined how to give a security instrument to the intra body correspondence. They utilized the lightweight single direction hash chain to build up the key. Tan et al. arranged a character based encryption (IBE) plot called IBE-Lite for the WBANs.

In any case, their conventions don't accomplish the start to finish security since everyone has two session keys; the one key is utilized to scramble information between sensor hub and nearby server, the other key is utilized to encode information between neighborhood server and AP. Moreover, the gathering key between sensor hubs and neighborhood server in [3] requires to be refreshed if there should arise an occurrence of hub cancellation or expansion.

3. SYSTEM OVERVIEW

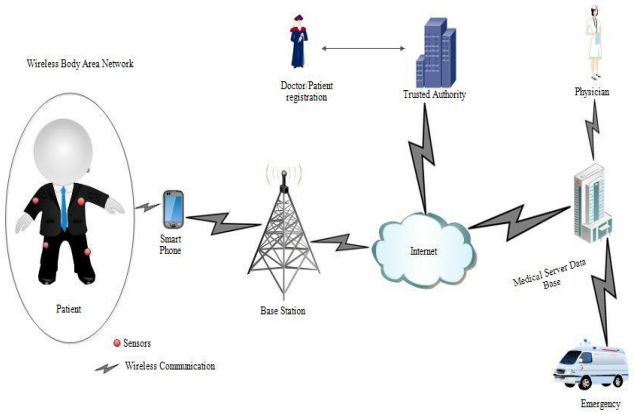

Fig. 1.WBAN Architecture

A common model of the proposed WBAN structure is in Fig. 1. The four huge components of the WBAN structure are trusted in power (TA), Sensors (usable and inserted), data sink (a phone like a propelled cell or the BAN data regulator), and customers, for instance, specialists, clinical masters and patients.

Sensors: Generally, a WBAN includes far off usable and introduced sensors. These are commonly used to give life support by checking basic normal body boundaries, for example, beat, inside warmth level, etc. The standard asset need of the embedded sensors is battery control showed up contrastingly corresponding to usable sensors. Since the contraptions are generally battery-fueled, the batteries can be feasibly empowered. Thusly, the information sink of the specific patient sends the regular data to a confirmed medicinal expert or an embraced ace intermittently.

Information Sink: An information sink is a remote, for example, a cell phone which is utilized to gather the common data from the introduced and wearable sensors. The information sink has correspondence and figuring capacities to convey the regular data to the supported stars. The information sink has the limit ability to store the aggregated trademark data and to store the enigma keys by TA , the hour of client's concealed enrolment process. The information sink can favor the accommodating aces or specialists in a cryptic way to get a handle on their validity with TA conveying the characteristic data to them. Obviously, ensuring the data in the information sink is in like way fundamental to keep up an indispensable decent ways from different classes of security assaults in WBANs. Therefore, the data kept in the information sink is ensured about and it isn't satisfactorily attacked by aggressors.

Clients and Confided in Authority (TA) are the other important parameters.

4. PROPOSED WORK

Trusted authority's initialization:

TA selects a random large prime number 'q' with it's multiplicative group *(Z_q*)* containing '*q-1*' elements.The secret keys of the TA are *'x'* and *'y'*. With the help of these keys, public keys ' A_1' and ' B_1' are calculated,

$$A_1 = g_1^x, \mathrm{B}_1 = g_1^{x+y}$$

Where g_1 is the generator or primitive root of ' q. Then TA selects a private key 'r' from Z_q*. The public key (pu_{TA})is calculated as $pu_{TA} = g_1^r$

Registration phase:
In registration process both patient and doctor has to enroll their personal details such as name, phone number, email id, aadhar id etc. During registration the patient as well as the doctor is provided with a private key 'α' and 'β' which is an element of Z_q* respectively.
Then they also receive the public keys (u_1 for patient and $d_1$for doctor) which are computed as

$$u_1 = g_1^{\alpha-y},\ \mathrm{d}_1 = g_1^{\beta+r}$$

TA provides {α ,u_1} and {β ,d_1} to the patient as well as doctor respectively.
Verification:

Verification is one of the major testing assignments. Unknown confirmation alludes to the component which guarantees and affirms client's character by methods for proper certifications. In this segment, we concentrate patient's confirmation just as specialist's verification.

Patient's Anonymous Authentication:

- $L_1 = u_1.g_1^{l_1+\alpha}$, $L_2 = g_1^{l_2+l_3}$, $L_3 = g_1^{l_2-l_1-\alpha}$

$$C = H(\ u_1||\ A_1||\ L_2||\ L_3)$$

Then, it computes L_1', L_2', L_3'.

$$L_1' = g_1^{-l_1}\ ,\ L_2' = g_1^{l_1+l_2+l_3}\ ,\ L_3' = g_1^{l_2-\alpha}$$
$$L_1'' = L_1'.L_1.B_1, L_2'' = L_2'.L_1'\ ,, L_3'' = L_1'.L_3$$

$$c'=H(u_1||L_1''||L_2''||L_3'')$$

Evidence of accuracy:

$$A_1 = L_1'', L_2 = L_2'', L_3 = L_3''$$

- $L_1'' = L_1'.L_1.B_1$

$= g_1^{-l_1}.g_1^{l_1-\propto}.g_1^{\propto-y}.g_1^{x+y}$
$= g_1^{-l_1+l_1-\propto+\propto-y+x+y}$
$= g_1^{x}$
$= A_1$

Thus,$A_1 = L_1''$

- $L_2'' = L_2'.L_1'$

$= g_1^{-l_1}.g_1^{l_1+l_2+l_3}$
$= g_1^{l_2+l_3}$
$= L_2'$

- $L_3'' = L_1'.L_3'$

$= g_1^{-l_1}.g_1^{l_2-\alpha}$
$= g_1^{l_1+l_2-\alpha}$
$= L_3$

Thus, $L_3 = L_3''$
Doctor's Anonymous Authentication:

- $m_1 = g_1^{k1-k2}$,$m_2 = g_1^{k_3-k_2}$,$\mathrm{m}_3 = \mathrm{d}_1.\mathrm{g}_1^{\mathrm{k}_1-\beta}$

$$c = H(d_1||pu_{TA}||m_1||m_2)$$

- $m_1' = g_1^{k_1+k_3-k_2}$,$m_2' = g_1^{-k_3}$,$m_3' = g_1^{-k_1}$
- $F_1'' = m_3.m_3'\ , m_1'' = m_1'.m_2'\ , m_2'' = m_1'.m_3'$

$c' = H(d_1||F_1''||m_1''||m_2'')$

Evidence of accuracy:

$$pu_{TA} = F_1'', m_1 = m_1'', m_2 = m_2''$$

- $F_1'' = m_3.m_3'$
  $= g_1^{k_1-\beta}.g_1^{-k_1}$
  $= g_1^{-\beta}.g_1^{\beta+r}$
  $= g_1^{r}$

Thus,$pu_{TA} = F_1''$

- $m_1'' = m_1'.m_2'$
  $= g_1^{k_3}.g_1^{k_1+k_3-k_2}$
  $= g_1^{k_1-k_2}$
  $= m_1$

Thus,$m_1 = m_1''$.

- $m_2'' = m_1'.m_3'$
  $= g_1^{-k_1}.g_1^{k_1+k_3-k_2}$
  $= g_1^{k_3-k_2}$
  $= m_2$

Thus,$m_2 = m_2''$

5. PERFORMANCE ANALYSIS

Here, we separate the display of the proposed arrangement with various plans

T_(add): It speaks to the time for point expansion activity.
T_exp : It speaks to the time for exponentiation activity.
T_h : It speaks to the time for hash work activity.
T_b : It speaks to the time for bilinear activity.
T_(mul): It speaks to the time for point activity.
T_s: It speaks to the time for symmetric encryption.

TABLE 1 : MANIPULATION COST OF VARIOUS SCHEMES

Method	For one user authentication	For n user authentication
Vijaya kumar et al.'s scheme	$2T_b + T_h + 4T_{mul} \approx 5.9ms$	$(n+1)T_b + nT_h + 4nT_{mul}$
Li et al.'s scheme	$5T_{mul} + 3T_h + 3T_s \approx 9.6ms$	$5nT_{mul} + 3nT_h + 3nT_s$
He et al.'s security scheme[7]	$4T_{mul} + T_{add} + 5T_h \approx 13.5ms$	$4nT_{mul} + nT_{add} + 5nT_h$
Liu et al.'s preliminary scheme[6]	$4T_{mul} + T_{add} + T_{exp} + 4T_h \approx 11.4ms$	$4nT_{mul} + nT_{add} + nT_{exp} + 4nT_h$

Proposed system (patient)	$3T_{exp} + T_h \approx 4.5ms$	$3nT_{exp} + nT_h$
Proposed system (doctor)	$3T_{exp} + T_h \approx 4.5ms$	$3nT_{exp} + nT_h$

All of the results are penniless down and a short time later the typical of the results is thought of. Here, the time boundaries T_exp and T_h are viewed as proportional to 0.6ms and 2.7ms independently.

6. CONCLUSION

Overall WBAN is used in the restorative field to give customized human amenities benefits and progress the idea of clinical by using usuale or implanted sensors. Vijaya kumar et al.'s scheme is $(n+1)T_b + nT_h + 4nT_{mul}$ is for n users. Li et al.'s scheme is $5nT_{mul} + 3nT_h + 3nT_s$ for n users. He et al.'s security scheme [7] is $4nT_{mul} + nT_{add} + 5nT_h$ is for n users. Liu et al.'s preliminary scheme [6] is $4nT_{mul} + nT_{add} + nT_{exp} + 4nT_h$ for n users. Proposed system for patient and doctor is $3nT_{exp} + nT_h$ for n users and the manipulation cost is considerably reduced

7. References

[1] J. Shen, S. Chang, J. Shen, Q. Liu, and X. Sun, "A lightweight multilayer authentication protocol for wireless body area networks," Future Gener. Comput. Syst., vol. 78, pp. 956–963, Jan. 2016.

[2] X. Li, M. H. Ibrahim, S. Kumari, and R. Kumar, "Secure and efficient anonymous authentication scheme for three-tier mobile healthcare systems with wearable sensors," Telecommun. Syst., vol. 67, no. 2, pp. 1–26, 2017.

[3] H. Debiao, S. Zeadally, K. N., and L. J.H., "Anonymous authentication for wireless body area networks with provable security," IEEE Systems Journal, vol. 11, no. 4, pp. 2590 – 2601, 2017.

[4] P. Vijayakumar, M. Azees, and L. Deboarh, "Cpav: Computationally efficient privacy preserving anonymous authentication scheme for vehicular ad hoc networks," in IEEE 2nd International Conference on Cyber Security and Cloud Computing, IEEE, 2016.

[5] C. Hu, H. Li, Y. Huo, T. Xiang, and Z. Liao, “Secure and efficient data communication protocol for wireless body area networks,” IEEE Transactions on Multi-Scale Computing Systems, vol. 2, no. 2, pp. 94–107,2016.

[6] Liu J , Zhang L , Sun R . 1-Raap: “An efficient 1-round anonymous authentication protocol for wireless body area networks”.Sensors2016;16:728.

[7] He D ,Wang D . “Robust biometrics-based authentication scheme for multiserver environment”. IEEE Syst J 2015;9:816–23 .

[8] B.Santhosh Kumar, Dr.S.Karthik, Dr.V.P.Arunachalam, " Upkeeping secrecy in Information Extraction using 'k' division graph based postulates", Cluster Computing, SpringerLink, ISSN:1386-7857, DOI: 10.1007/s10586-018-1705-2, Volume 22, Supplement 1, pp 57–63, January 2019, Pages:1-7

[9] R.Cristin, B. Santhosh Kumar, C. Priya, K. Karthick " Deep neural network based Rider-Cuckoo Search Algorithm for plant disease detection", Artificial Intelligence Review (Springer), https://doi.org/10.1007/s10462-020-09813-w, Pages: 1-26