Available online at: http://brsj.cepsbasra.edu.iq

ISSN -1817 -2695

DESIGN A LIGHTWEIGHT AUTHENTICATION SCHEME FOR WBAN IN HEALTHCARE SYSTEMS

[1]YASAMEEN A. MUHSIN, [2]ALI A. YASSIN

[1]*Computer Science Dept., College of Education for Pure Sciences, Basrah University*

[2]*Computer Science Dept., College of Education for Pure Sciences, Basrah University*

E-mail: [1]jasminasadi933@gmail.com, [2]aliadel79yassin@gmail.com

ABSTRACT

The widespread and attractive use of smart devices in recent years has made it possible to use them in many aspects of human life such as health care. Wireless Body Area Network (WBAN) is a network made up of small sensors that collect vital signals from the human body to the personal device that could be a mobile phone used in health care systems. WBAN considers can an integrated network with mobile phone to give health services to the patients. This type of network is requiring building strong security scheme to resist various malicious attacks. In this paper, we focus to build strong and lightweight authentication scheme and depends on mobile phone to deal and follow the patients' cases. The proposed scheme resists malicious attacks such as Man-In-The-Middle (MITM), replay, and Denial of service (DoS) attacks. Our work also supports many features like mutual authentication, key management, anonymity, mobile health care. Also, the cost of the proposed scheme is an efficient in terms of computation and communication. In addition, the formal analysis using AVISPA tool proven the security of our scheme.

Keywords: *WBAN, Authentication, Malicious attacks, Mobile health care, AVISPA.*

1. INTRODUCTION

Healthcare systems allow the provision of health services more easily and comfortably for the patient. Where modern technology has contributed to reducing the financial costs of healthcare, as it is now possible to check a patient's health conditions remotely, thus avoiding hospitalization [1, 2].

With the need to have applications that support healthcare, type of networks, known as a Wireless Body Area Network (WBAN) has emerged. This network allows the exchange of health information between scientists, the reduction of the therapeutic cost, and providing health care remotely [3]. Generally, WBAN consists of tiny devices called sensors that can collect vital signals from the human body like blood pressure level, blood sugar level, and body temperature. The personal digital assistant, which may be a smartphone or a personal computer that can receive signals from the sensor. The service provider or server that contains the database [4-6].

However, security and privacy problems are among the most important challenges facing the WBAN. Patient data is personal and sensitive information transmitted over a wireless channel during the communication process, therefore it is subject to various attacks, which may be harmful to the patient and threaten his life [7, 8]. So we must take into account the privacy and security aspects when designing a scheme for the WBAN environment. For the purpose of privacy and confidentiality of the data we used a Blowfish encryption algorithm which provides more security, it is also fast and simple. Figure 1 shows the WBAN in the healthcare system.

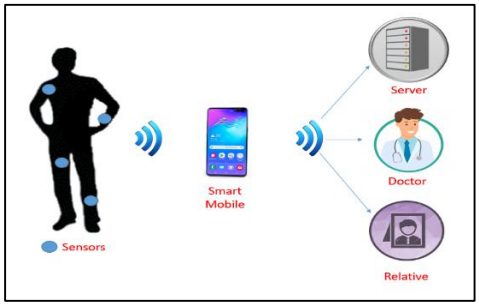

Figure 1: WBAN in the Healthcare System

1.1 Our Contributions

We can summarize the main contributions of the proposed scheme as follows:

- Proposed a new lightweight authentication scheme based on the ECC cryptosystem, can achieve features like mutual authentication and user anonymity, as well as, resistant MITM, DoS, and replay attack.
- The proposed scheme mainly supports healthcare, as it focuses on conserving the sensor energy and responding quickly to emergencies.
- Designing a smartphone application that can interpret the vital signal, warn the patient, and contact the attending physician in an emergency.
- Performance analysis shows the proposed scheme is efficient and provides low cost for computation and communication.

1.2 Organization

The rest of this paper is organized as follows: Section 2 presents the related work. Section 3 illustrates preliminaries which include Blowfish algorithm and SHA-512. Section 4 explains scheme components. Section 5 explains the proposed scheme and its four phases. Section 6 presents security and performance analysis, with the comparison with related work. Finally, section 7 summarize the conclusion.

2. RELATED WORK

In this section, we have provided some previous work in the field of WBAN and healthcare in recent years.

In 2011 Eldefrawy et al. [9] suggested designing a protocol that supports adding new nodes and canceling nodes within the network. The proposed protocol based on RSA and DHECC cryptosystems, and it provides security requirements. In 2013 Ramli et al. [10] proposed a scheme to protects health information during the communication based on the biometric signals ECG. The scheme shows the ability to use biometric signals as a secret key for the encryption process which provides a low cost for authentication. In 2014 Lee et al. [11] suggested an efficient scheme for key management based on ECC cryptography to protects the patient's health information. The researchers used the SIM card number of the patient as an identification number next to the private key. In 2016, Shin et al. [12] proposed an authentication protocol to resolve the drawback of Khan et al.'s protocol [13]. The new protocol provided a dynamic identity for each session, which was based on a random number. Shen et al. [14] presented an efficient protocol based on multilayer authentication and certificatless cryptography by using an ECC algorithm that offers improved security and a reduction in the computational cost. Ibrahim et al. [15] proposed a new protocol that maintains the anonymity of the sensors and the confidentiality of the data transmission. The researchers explain that, to meet security requirements, where the authentication alone is not sufficient even if the data is encrypted. In 2017, Wei et al. [16] designed an anonymous authentication scheme based on a low-entropy password. The researchers consider their scheme to be more suitable for WBAN because it relies on an easy-to-remember password. Li et al. [17] proposed a one-round authentication protocol to overcome the problems in Liu et al.'s protocol [18], and the results of the comparison proved that Li et al.'s proposed protocol resisted more attacks than Liu et al.'s protocol, even though they cost the same amount. In 2018 Chen et al. [19] presented a new authentication scheme to address security problems in Li et al.'s protocol [20], the proposed scheme has achieved high effectiveness in wireless sensors and mobile phones. The safety of the scheme is proven using the verification tool Proverif. Koya and P.P. [21] provided a hybrid scheme for mutual authentication and anonymity using physiological signals which helps to secure the scheme against sensor node impersonation attacks, as well as other attacks. This scheme outperforms other similar schemes in terms of computation, communication, and various safety functions. In 2019, Liu et al. [22] presented a new authentication scheme that was distinct from other schemes, as it used a dynamic password instead of a static password. The researchers used a computation algorithm to generate a unique password for each login. Kumar et al. [23] designed an authentication scheme based on the ECC cryptosystem for wearable devices suitable in the WBAN environment, this protocol has achieved good results in terms of security requirements and communication costs.

In order to contribute to this promising field, we proposed an authentication scheme for the WBAN environment that focuses on healthcare and provides security features and requirements. In addition to designing a mobile application that is able to take quick action in emergency situations. Formal analysis using AVISPA and security analysis demonstrated the superiority of the proposed scheme over related works in terms of security and productivity. (See Table 2).

3. PRELIMINARIES

3.1 Blowfish Algorithm

Blowfish is a symmetric cryptosystem algorithm designed by Bruce Schneire, has good traits like fast, compact, simple, and variably secure. Blowfish consists of two parts; first part is key expansion which convert the key into a sub keys array with total 4168 bytes. The second part is data encryption which consists of process iterated 16 times. Blowfish using simple operations such as addition and XOR operations [24].

3.2 Secure Hash Algorithm

Secure Hash Algorithm (SHA-512) developed in 1993 by NSA, and it is the final version of SHA-224 and SHA-256, takes inputs of variable length, and output a hash code with a length of 512 bits. SHA-512 uses a 64 bits word with 80 rounds, its guarantees the integrity of data and provides more security, but not time efficient. [25, 26].

4. SCHEME COMPONENTS

Three main components are the basis for WBAN which are the Sensor, the Smart Mobile, and the Service Provider detailed as follows:

1. **Sensor:** Is a tiny device with limited resources suitable for collecting vital signals from the human body.

2. **Smart Mobile:** Is a personal phone attached with the patient all the time and ready to receive vital signals.

3. **Service Provider:** A server gives the services to the users and has a database used to store patients' health records.

Table 1: Paper Notations

Notation	Description
S_i	Sensor
SM_i	Smart Mobile
SP	Service Provider
ID_i	User Identity
PW_i	User Password
TID_i	Temporary User Identity
TPW_i	Temporary User Password
C_i	Server Challenge
ID_{S_i}	Sensor Identity
TID_{S_i}	Temporary Sensor Identity
r_i	Random Number
$\oplus$	XOR Operation
$h\,(\,)$	Hash Function

5. OUR PROPOSED SCHEME

Our proposed scheme consists of four phases: registration phase, login phase, authentication phase, and healthcare phase. In the first phase, the user can use application in Smart Mobile (SM_i) to register on the Service Provider (SP). On the other side, Sensor (S_i) must be linked to target user (patient) and connect an identity with patient's identity. The login and authentication phases will be detailed later. We focus on the healthcare phase where the safety of the patient is the most important.

5.1 Registration Phase

First: The steps of SM_i registers:

- User selects identity (ID_i) and password (PW_i).
- The SM_i compute temporary parameters:
  - $TID_i = h\ (ID_i)$
  - $TPW_i = h\ (PW_i)$
- SM_i sends (TID_i, TPW_i) to SP.
- SP checks the validity of (TID_i, TPW_i) in its database to accept or reject the user.
- If the user accepted, then SP computes a challenge $C_i = h\ (TID_i \oplus TPW_i)$ and sends it to the user.

Second: The SM_i register S_i by selecting a random identity for sensor ID_{S_i} and sends it to S_i for saving in its memory. Figure 2 shows the registration phase.

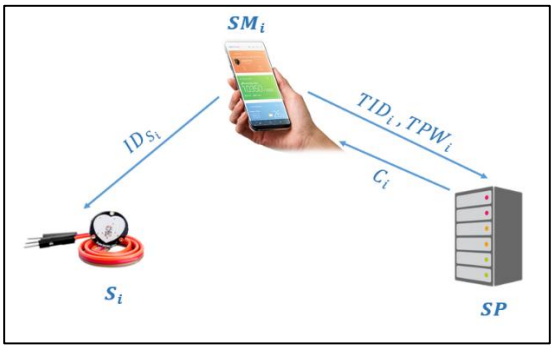

Figure 2: Registration Phase

5.2 Login Phase

First: S_i picks a random number r_i and computes temporary $TID_{S_i} = ID_{S_i} \oplus r_i$ and sends $(TID_{S_i},\ r_i)$ to SM_i.

Second:

- User enters ID_i and PW_i on the SM_i interface.
- SM_i computes temporary $TID_i = h(ID_i)$ and $TPW_i = h(PW_i)$.
- SM_i encrypts TID_i and TPW_i using Blowfish algorithm.
- SM_i selects random number r_i and computes $TID_i^* = TID_i \oplus r_i$ and $TPW_i^* = TPW_i \oplus r_i$ and sends (TID_i^*, TPW_i^*, r_i) to SP. Figure 3 shows the login phase.

5.3 Authentication Phase

First: The SM_i verifies S_i by calculating $TID_{S_i}^* = ID_{S_i} \oplus r_i$, and checks if $TID_{S_i}^* = TID_{S_i}$ then SM_i accepts the login request.

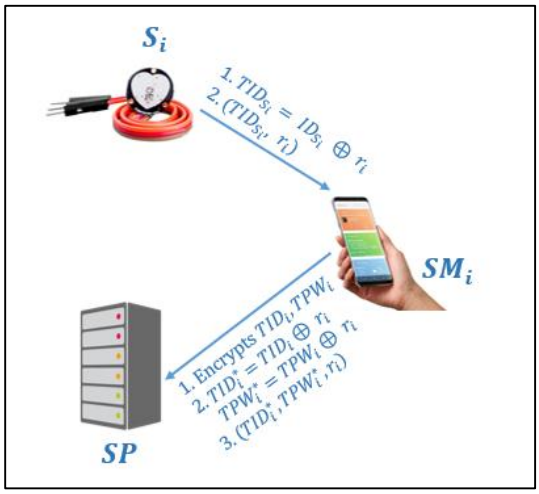

Figure 3: Login Phase

Second: The SP verifies user by following steps:

- Computes $TID_i^{**} = TID_i^* \oplus r_i$ and $TPW_i^{**} = TPW_i^* \oplus r_i$.
- Decrypts TID_i^{**} and TPW_i^{**} using Blowfish algorithm.
- Checks if $(TID_i^{**} = TID_i)$ and $(TPW_i^{**} = TPW_i)$.
- Selects random number r_i and encrypts C_i using Blowfish algorithm and computes $C_i^* = C_i \oplus r_i$ and sends (C_i^*, r_i) to SM_i.
- On the other side SM_i computes $C_i^{**} = C_i \oplus r_i$ and decrypts C_i^{**} using Blowfish algorithm, then checks if $C_i^{**} = C_i$, the mutual authentication process is successful if all the above parameters are equal. Figure 4 shows the authentication phase.

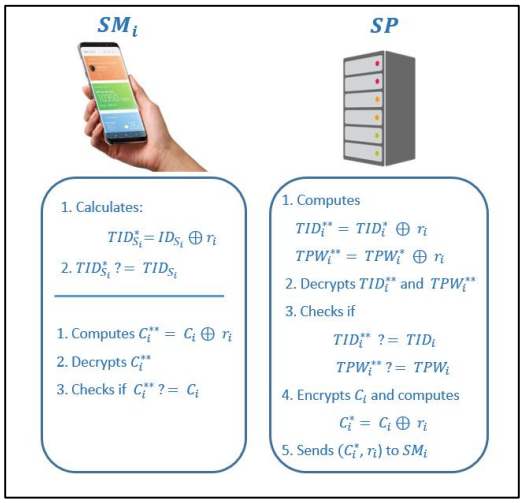

Figure 4: Authentication Phase

5.4 Healthcare phase

At this phase, the focus is on the patient in particular, as this phase is concerned with the way of providing health services to the patient and taking great care of the patient's life first. This phase works in two ways:

1. The first way is to takes full advantage of the limited sensor energy for the longest possible period, where specific times can be specified to send the vital signal from S_i to SM_i and divide the signal into two types normal and abnormal.

2- The second method is towards designing a smart phone application that effectively contributes to making the patient aware of the developments of his health, warning the patient directly when an abnormal signal occurs, and informing the physician in emergency cases.

6. ANALYSIS

6.1 Security Analysis

1. Mutual Authentication:

Our proposed scheme supports mutual authentication between SM_i and SP. For each login process, both parties must verify the other's credibility through a set of steps mentioned in the authentication phase.

2. User Anonymity:

When the user enters the ID_i and PW_i on the applications' interface for the purpose of logging in, the SM_i converts it to hash code by using SHA-512 hash function before sending it to the SP, in addition, the identity and password stored in the SP are the output of SHA-512 (TID_i, TPW_i), which ensures that the true user ID_i is hidden.

3. S_i Impersonation Attack:

The sensor impersonation attack can successful when the adversary Å creates a valid TID_{S_i} and sends it with a random r_i. However, this type of attack fails because TID_{S_i} should be computed from the original ID_{S_i}.

4. MITM Attack:

We assume that Å can obtain the exchanged messages (TID_{S_i}, r_i), (TID_i, TPW_i, r_i), and (C_i, r_i) between S_i, SM_i, and SP during login and authentication phases. Å changes these messages and sends it to the legal party, these messages cannot exceed the verification step because Å does not posse the real parameters.

5. Replay Attack:

In this type of attack, Å tries to obtain the message and re-send it more than once. Also, this type fails in our scheme due to the use of random numbers besides using a Blowfish algorithm, which makes the message changing every time.

6. DoS Attack:

All messages exchanged (TID_{S_i}, r_i), (TID_i, TPW_i, r_i), and (C_i, r_i) between the components of the proposed scheme (S_i, SM_i, SP) during the login and authentication phases are generated once due to r_i when connect between S_i and SM_i, and Blowfish encryption during connect between SM_i and SP, so Å cannot floods the network with a flood of duplicate messages because it will be rejected.

7. Stolen SM_i :

The Å cannot use the stolen SM_i to resend old messages because our scheme is safe against a replay attack. Also, it is not possible to falsify new health information, due to a break in his connection with S_i after a certain distance.

Table 2 shows the security features comparison, where F1: Mutual Authentication, F2: User Anonymity, F3: S_i Impersonation Attack, F4: MITM Attack, F5: Replay Attack, F6: DoS Attack, F7: Stolen SM_i, and F8 Healthcare Phase.

Table 2: Security Features Comparison

Features	Schemes			
	Our	[15]	[21]	[22]
F1	Yes	Yes	Yes	Yes
F2	Yes	Yes	Yes	Yes
F3	Yes	Yes	Yes	Yes
F4	Yes	Yes	Yes	No
F5	Yes	Yes	Yes	Yes
F6	Yes	No	No	No
F7	Yes	No	No	No
F8	Yes	No	No	No

6.2 Performance Analysis

The computational cost of the proposed scheme and the related works is calculated based on the cost of the hash function which requires 0.0023 ms [27]. While the communication cost during login and authentication phases is calculated by assuming 128 bits size for each of identity and password, the output of a hash function is 512 bits, and the size of the random numbers is 32 bits. Figure 5 shows the comparison of the computation and communication costs of the proposed scheme with related works.

6.3 Formal Analysis

In order to prove the security of the proposed scheme in a formal way, we used a robust verification tool used to verifier if the scheme is secure or not.

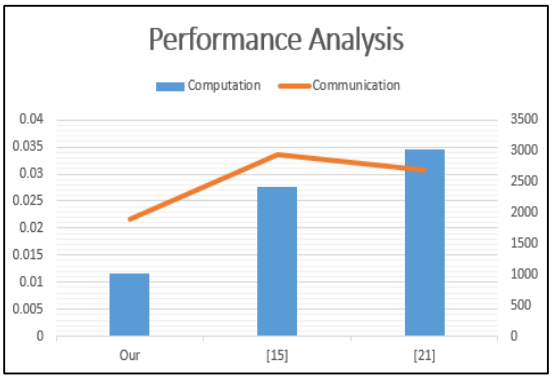

Figure 5: Computation and Communication Costs

This tool called Automated Validation of Internet Security Protocols and Applications (AVISPA) [28]. The results of the simulation shows that the proposed scheme is safe against the malicious attacks.

7. CONCLUSION

In this paper, we proposed a lightweight authentication scheme for the WBAN environment. Our work is interested in providing healthcare services for the patient in a better way with the help of the smart phone application. Additionally, the proposed scheme supports security features such as mutual authentication and anonymity, as well as, resistant the well-known attacks like MITM, DoS, and replay attacks and this was proven using the simulation tool AVISPA. Performance analysis shows the efficiency of the proposed scheme in computation and communication costs. The proposed scheme outperforms the related work in terms of resistance to attacks and achievement.

REFERENCES

[1] M. M. Dhanvijay and S. C. Patil, "Internet of Things: A survey of enabling technologies in healthcare and its applications," *Computer Networks,* vol. 153, pp. 113-131, 2019.

[2] P. Brous, M. Janssen, and P. Herder, "The dual effects of the Internet of Things (IoT): A systematic review of the benefits and risks of IoT adoption by organizations," *International Journal of Information Management,* vol. 51, p. 101952, 2020/04/01/ 2020.

[3] R. Negra, I. Jemili, and A. Belghith, "Wireless Body Area Networks: Applications and Technologies," *Procedia Computer Science,* vol. 83, pp. 1274-1281, 2016.

[4] G. V. Crosby, "Wireless Body Area Networks for Healthcare: A Survey," *International Journal of Ad hoc, Sensor & Ubiquitous Computing,* vol. 3, pp. 1-26, 2012.

[5] R. A. Khan and A.-S. K. Pathan, "The state-of-the-art wireless body area sensor networks: A survey," *International Journal of Distributed Sensor Networks,* vol. 14, 2018.

[6] Safina Shokeen and D. Parkash, "A Systematic Review of Wireless Body Area Network," presented at the International Conference on Automation, Computational and Technology Management (ICACTM) Amity University, 2019.

[7] P. Niksaz, "Wireless Body Area Networks: Attacks and Countermeasures," *International Journal of Scientific & Engineering Research,,* vol. 6, September 2015.

[8] S. Al-Janabi, I. Al-Shourbaji, M. Shojafar, and S. Shamshirband, "Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications," *Egyptian Informatics Journal,* vol. 18, pp. 113-122, 2017.

[9] M. H. Eldefrawy, M. K. Khan, K. Alghathbar, A. S. Tolba, and K. J. Kim, "Authenticated key agreement with rekeying for secured body sensor networks," *Sensors (Basel),* vol. 11, pp. 5835-49, 2011.

[10] Sofia Najwa Ramli, Rabiah Ahmad, Mohd Faizal Abdollah, and E. Dutkiewicz, "A Biometric-based Security for Data Authentication in Wireless Body Area Network (WBAN)," pp. 998-1001, 2013.

[11] Young sil Lee, Esko Alasaarela, and H. Lee, "Secure Key management Scheme based on ECC algorithm for Patient's Medical Information in Healthcare System," *IEEE Access,* pp. 453-457, 2014.

[12] S. Shin, S. W. Lee, and H. Kim, *Authentication Protocol for Healthcare Service over Wireless Body Area Networks* vol. 5. International Journal of

Computer and Communication Engineering, 2016.

[13] K. Khan and S. Kumari, "An Improved User Authentication Protocol for Healthcare Services via Wireless Medical Sensor Networks," *International Journal of Distributed Sensor Networks,* vol. 2014, pp. 1-10, 04/26 2014.

[14] J. Shen, S. Chang, J. Shen, Q. Liu, and X. Sun, "A lightweight multi-layer authentication protocol for wireless body area networks," *Future Generation Computer Systems,* vol. 78, pp. 956-963, 2016.

[15] M. H. Ibrahim, S. Kumari, A. K. Das, M. Wazid, and V. Odelu, "Secure anonymous mutual authentication for star two-tier wireless body area networks," *Comput Methods Programs Biomed,* vol. 135, pp. 37-50, Oct 2016.

[16] F. Wei, P. Vijayakumar, J. Shen, R. Zhang, and L. Li, "A provably secure password-based anonymous authentication scheme for wireless body area networks," *Computers & Electrical Engineering,* vol. 65, pp. 322-331, 2017.

[17] X. Li, J. Peng, S. Kumari, F. Wu, M. Karuppiah, and K.-K. Raymond Choo, "An enhanced 1-round authentication protocol for wireless body area networks with user anonymity," *Computers & Electrical Engineering,* vol. 61, pp. 238-249, 2017.

[18] J. Liu, L. Zhang, and R. Sun, "1-RAAP: An Efficient 1-Round Anonymous Authentication Protocol for Wireless Body Area Networks," *Sensors,* vol. 16, p. 728, 05/19 2016.

[19] C.-M. Chen, B. Xiang, T.-Y. Wu, and K.-H. Wang, "An Anonymous Mutual Authenticated Key Agreement Scheme for Wearable Sensors in Wireless Body Area Networks," *Applied Sciences,* vol. 8, p. 1074, 2018.

[20] X. Li, M. H. Ibrahim, S. Kumari, A. K. Sangaiah, V. Gupta, and K.-K. R. Choo, "Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks," *Computer Networks,* vol. 129, pp. 429-443, 2017/12/24/ 2017.

[21] A. M. Koya and D. P. P, "Anonymous hybrid mutual authentication and key agreement scheme for wireless body area network," *Computer Networks,* vol. 140, pp. 138-151, 2018.

[22] X. Liu, R. Zhang, and M. Zhao, "A robust authentication scheme with dynamic password for wireless body area networks," *Computer Networks,* vol. 161, pp. 220-234, 2019.

[23] D. Kumar, H. S. Grover, and Adarsh, "A secure authentication protocol for wearable devices environment using ECC," *Journal of Information Security and Applications,* vol. 47, pp. 8-15, 2019.

[24] M. W. Munir. (2005). *Cryptography*. Available: https://www.researchgate.net/publication/276317739

[25] C.G Thomas and R. T. Jose, "A Comparative Study on Different Hashing Algorithms," *International Journal of Innovative Research in Computer and Communication Engineering,* vol. 3, pp. 170-175, 2015.

[26] D Rachmawati, J T Tarigan, and A. B. C. Ginting, "A comparative study of Message Digest 5(MD5) and SHA256 algorithm," presented at the International Conference on Computing and Applied Informatics, 2017.

[27] H. H. Kilinc and T. Yanik, *A Survey of SIP Authentication and Key Agreement Schemes* vol. 16. IEEE COMMUNICATIONS SURVEYS & TUTORIALS, 2014.

[28] Y. Glouche, T. Genet, O. Heen, and O. Courtay. (2006). *A Security Protocol Animator Tool for AVISPA*. Available: https://www.researchgate.net/publication/228356197

تصميم مخطط مصادقة خفيف الوزن لشبكة WBAN في أنظمة الرعاية الصحية

[1] ياسمين عباس محسن، [2] علي عادل ياسين

[1]قسم علوم الحاسوب ، كلية التربية للعلوم الصرفة ، جامعة البصرة
[2]قسم علوم الحاسوب ، كلية التربية للعلوم الصرفة ، جامعة البصرة
البريد الالكتروني: [1]jasminasadi933@gmail.com, [2]aliadel79yassin@gmail.com

الخلاصة:
الاستخدام الواسع والجذاب للأجهزة الذكية في السنوات الأخيرة جعل من الممكن استخدامها في العديد من جوانب الحياة البشرية مثل الرعاية الصحية. الشبكة اللاسلكية لمنطقة الجسم (WBAN) هي شبكة تتكون من أجهزة استشعار صغيرة تجمع إشارات حيوية من جسم الإنسان وترسلها إلى الجهاز الشخصي الذي يمكن أن يكون هاتفًا محمولًا او حاسبة شخصية. WBAN يمكن ان تكون مع الهاتف المحمول شبكة متكاملة لتقديم الخدمات الصحية للمرضى. يتطلب هذا النوع من الشبكات بناء مخطط أمني قوي لمقاومة الهجمات الخبيثة المختلفة. في هذه الورقة ، نركز على بناء نظام مصادقة قوي وخفيف الوزن ويعتمد على الهاتف المحمول للتعامل مع حالات المرضى ومتابعتها. يقاوم المخطط المقترح الهجمات الخبيثة مثل هجمات Man-In-The-Middle (MITM) وإعادة التشغيل ورفض الخدمة (DoS). يدعم عملنا أيضًا العديد من الميزات مثل المصادقة المتبادلة وإدارة المفاتيح وإخفاء الهوية والرعاية الصحية المتنقلة. كما أن تكلفة المخطط المقترح فعالة من حيث الحساب والاتصال. بالإضافة إلى ذلك ، أثبت التحليل الرسمي باستخدام أداة AVISPA أمان مخططنا.

الكلمات الرئيسية: WBAN ، المصادقة ، الهجمات الخبيثة ، الرعاية الصحية المتنقلة ، AVISPA.