Distributed Data Security and Privacy in WBAN-Related e-Health Systems

Asst.Prof. Dr.Sufyan T. Faraj*, Lecturer Dr.Ali J. Dawood*, Abeer D. Salman*

Abstract

The wireless body area network (WBAN) has emerged as a new technology for e-healthcare that allows the data of a patient's vital body parameters and movements to be collected by small wearable or implantable sensors and communicated using short-range wireless communication techniques. WBAN has shown great potential in improving healthcare quality, and thus has found a wide range of applications. However, the security and privacy protection of the data collected from a WBAN, either while stored inside the WBAN or during their transmission outside of the WBAN, is a major unsolved concern. Challenges are mainly coming from stringent resource constraints of WBAN devices. The aim of this work is to achieve secure and dependable distributed data storage in the WBAN. At the first part of the paper, we will survey the most recent research directions in the field.Significant recent papers are discussed and compared to each other to identify the advantages and disadvantages of each technique. Then, our proposed strategy will be devoted based on that survey. The proposal is mainly based on the techniques of erasure coding, secret sharing and an algebraic signature to simultaneously achieve data confidentiality, dependability, and dynamic integrity.

Keywords: WBAN , e-Healthcare,Short-Rang wireless communication

*College of Computer, University of Anbar

1. Introduction

The term "Wireless Body Area Network"was introduced by Van Dam et al. in 2001 [1].WBAN is considered a promising technique thatcan improvehealthcarein general and especially "*e-health systems"* [2]. WBAN consists of small and intelligent devices (nodes). These devices are attached on or implanted in the human body. Using this network, the patients' parameters,such asvital signs (heart rate, blood pressure, oxygen saturation, etc.) or environmental parameters (location, temperature, humidity, light, etc.),can be monitored remotely, continuously, then processed and transferred to medical databases [3]. There are two typesfor storingpatient's data. The first is centralized storage. This kind is simple; however, it can lead to a single point of failure [4],such as if we store confidential data in one server. If that server failed (or compromised), the result may be loss or damage of all information. Also, the case of network disconnections may prevent any neighborhood servers from accessing data for long periods. Hence, using this type of storageusually cannot offer the level of dependability or availability as required by e-health systems. Therefore, to ensure these security and operational requirements,it is preferred to use the second type of data storage which implies that the storage must be distributed and redundant [5].

Healthcare networks face many different types of attacks or threats. Depending on the intended target, the attacks can be categorized into eavesdropping, modification, masquerading, etc. These attacks are on the patient nodes. Other types of attack such as Denial-of-Service (DoS) and system intrusion are attacks on the healthcare system that aims to damage the connection between the medical personnel and the patient nodes. They also can be launched to destroy the central system itself [6]. the security and privacy of patient's information are considered essential components for the system security of the WBAN. The meaning of data security is that the data is securely stored and transferred while data privacy means the data can only be accessed by the people who have authorization to show and use them [2].

The aim of this work is to propose a system for secure distributed data storage in WBAN-based e-health applications. The system relies on encoding data through the integration of theRedundant Residue Number System(RRNS) technique and (public-key based) digital signatures to achieve confidentiality, dependability, integrity, and authentication. The remaining of this paper is organized as follows: Section 2 outlines characteristics and challenges of WBANs emphasizing on security requirements. Next, Section 3 represents a literature survey of significant related work. The Redundant Residue Number System (RRSN) technique is reviewed in Section 4. Then, the proposed system main phases are described in Section 5. Finally, the paper is concluded in Section 6.

2. Wban Characteristics and Challenges

The main characteristics of WBAN compared to another network are [1]*:*

1. WBANs are consideredas small-scale networks, and they have short communication range not to exceeding in or on a human body.
2. To minimize interference and to cope with health concerns; extremely low transmit power per node is needed.
3. High reliability and low delay is required; because the data mostly consists of medical information.

4. The topology of WBAN is "star topology", where communication centrally organized and every sensor node is directly linked to a master node. This topology cannot always meet the desired reliability requirement therefore a star-mesh hybrid topology extends the conventional approach and creates mesh networking among central coordinators in multiple star networks [7].

The generic architecture of WBANsconsists ofthree layers.*Medical server* is the top layer; this server encompass a healthcare professionals. The basic function of the medical server is to keep electronic medical records of registered patient and provide variousservices to the users and medical personnel. The nextlayer is the *personal server* that has many functions like interfacing WBAN sensor nodes, providing the graphical user interface, and communicating with services at the top layer. The personal server employs mobile telephone networks (2G, GPRS and 3G) or WLANs to communicate with the medical server. The third layer consists of a number of intelligent nodes, each*sensor node* receives initialization commands and responds to queries from the personal server. The main functions of these sensor nodes are to sample vital signs and transfer the relevant data to a personal server. They do this by using wireless personal network implemented using ZigBee (802.15.4) or Bluetooth (802.15.1) [3]. Figure 1 explains the general architecture of a WBAN.

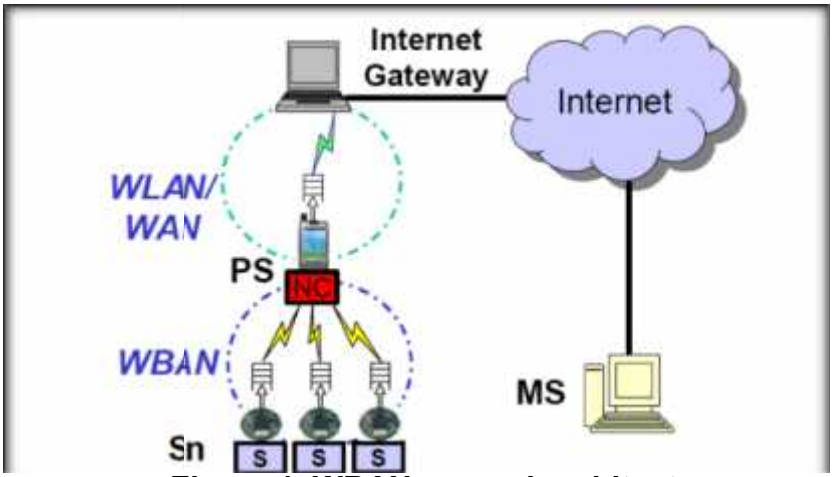

Figure 1. WBAN general architecture.

There are still many challenges related to WBANs research and deployment. The most important challenges that appear in WBANs are as follow [7], [8]:

- Network topology: The topology of this network is more variable due to body movement therefor WBANs should be robust against frequent topology changes.
- Node replacement: There are difficulties in the replacement of implanted nodes.
- Node lifetime: It is quite desirable to have long lifetime of the devices like several years/months especially for implanted devices. However, it can be impossible to recharge or change the batteries for most devices. Hence, the energy resources, the computational power and available memory of such devices are limited.

- Security level: To make the patient's information strictly private and confidential, the security level must be higher and stringent security mechanisms are required.

The issues of security and privacy are crucial for WBAN applications. Wheneverit is decided to use distributed data storage in WBANs in order to offer availability and dependability, the most important security requirements that must be meet are [2]:

- *Authentication:*This ensures that the sender of the patient-related data is authenticated, and it must prevent inserting any data from outside the WBAN.
- *Confidentiality:* It protects data from an illegal user. The common method that used to provide data confidentiality is"Encryption". The amount of confidentiality can be determined depending on the type of cipher scheme and mode of operation [9].
- *Integrity*: This service guarantees the correctness of data, protecting against modification, deletion, creation and replication from an unauthorized user. The methods that are providing data integrity are MD (Message Digest) and MAC (Message Authentication Code) [10].
- *Dependability*: Whena node is failed or data erasure happens, the data of patient must be readily retrievable.In order to enhance the dependability of the data,methods that provide redundancy are used.

3. Literature Survey

In this section, asurveyof some important related works that deals with data storage in WBANs is presented.These worksare compared and discussed to verify whether they can satisfy the previous requirements. This can facilitate the envision of potential future directions.

In 1989, Rabin[11] proposed atechnique for fault-tolerant file server that usean Information Dispersal Algorithm (IDA) to break a file into$n$ pieces so that every m pieces are sufficient for reconstructing file. Storing copies of file at other network nodes might be a solution for loss of a file but this canincrease storage in the system. The case of failure required retransmitting file along a different pathwhich caused a loss in time.IDA disperses the information of file into n pieces or locations in reliable way. The file can be reconstructed from any m pieces. The main advantage ofthis dispersal method is space efficiency. Both of the dispersal and reconstruction are computationally efficient. Themain disadvantageof IDA isthat it did not address the confidentiality issues.

In 2003, Chessaand Maestrini[5] proposed a method for distributed storage by using RRNS to encode the file. The advantage of RRNS is that this technique has the ability to detect any error up to multiplicity R and has the ability to correct any error up to multiplicity $[\frac{R}{2}]$. This system achieve the Dependability since data can be reconstructed in the presence of up to$s \leq R$residue erasures, combined with up to$(R-s)/2$corrupted residues. It also ensures data confidentiality since recovering the original information requires knowledge of the all modules (keys). However, this scheme lacks authentication and integrity capabilities.

In 2005, Subbiahand Blough [12] proposedto use a distributed set of storage servers for storing sensitive information. If some storage servers are compromised, the confidentiality, integrity, and availability requirements of the sensitive data that are storedin these servers must still be met.This approach uses integration of XOR

secret sharing and replication mechanisms, which minimize the computation overheads and achieve speeds comparable to standard encryption schemes. Thenature of collaborative work environments allows multiple authorized clients to access the encrypted data. Secret sharing schemes encode data intoshares. Whenit is required to reconstruct the encoded data, it would be needed to combine certain valid shares. Perfect secret sharing schemes have the feature that the shares can be changed, or "renewed", distributively such that the encoded data still remain the same. This featurecan provide strong data confidentiality. However,most perfect secret sharing schemes have high computational cost.

In 2007, Subramanian et al [13] used three schemes to deal with securing stored information.The objective of theirworkwas to prevent attackers from decoding (interpreting) the captured data. Theproposed schemes werefor securing both distributed data storage and retrieval. The first of these schemecalled a Simple Hash-Based (SHB) supports distributed data storage but relies on a centralized entity for data retrieval. Because ofthe limitations of this scheme, a second scheme called Enhanced Hash-Based (EHB) was introduced. It also can secure both distributed data storage and distributed data retrieval. In EHB scheme, secret keying information is preloaded to sensor nodes and authorized users, and then they can perform distributed data storage and retrieval without the involvement of any centralized entity. However, the EHB scheme imposes strict restrictions on the network.Thus, they proposed a third scheme called Adaptive Polynomial-Based (APB) scheme to solve the limitation of non-scalability in the EHB scheme. The APB scheme allows a network controller on demand to refresh the keying information stored in sensor nodes and thus provide better scalability and flexibility.

In 2009, Wang et al [4] proposed a scheme to achieve security, dependability, and dynamic integrity in data storage. In the initial data storage process, they utilized perfect secret sharing and erasure coding to guarantee data confidentiality and dependability. A weak point of this scheme is that it does not allow a third party to carry out integrity checks. This is quite unsuitable in WBAN applications because it is quite desirable in such applications that the local server to verify the integrity of the collected data.

4. Redundant Residue Number System (RRNS)

This section represents a review of some important cryptographic methods used in developing the proposed system. Our proposal is mainly based on integrating the RRNS technique for achieving distributed data confidentiality with the public-key based RSA and DSA algorithms to achieve authentication and integrity. The procedure of the RSA algorithm for encrypting and decrypting messages can be found in [14]. The Digital Signature Algorithm (DSA) uses a hash function to prove that the message has not been modified during storing or transmission. More details about this issue can be found in [14] and [15].

Here, more attention is given to the RRSN technique. This technique depends on choosing $(T+R)$ pairwise prime, positive integers $m_1, m_2, \ldots\ldots, m_T, m_{T+1}, .., m_{T+R}$ **where**

$$M = \prod_{i=1}^{T} m_p \quad (1)$$

$$M_k = \prod_{p=T+1}^{R} m_p \quad (2)$$

For non-negative integer X, the residues of X modulo mp can be found by:

$$x_p = X \bmod m_p. \quad (3)$$

The **(T+R)-tuples** $(x_1,..,x_{T+R})$ is called residue representation of ***X***. In order to reconstruct ***X*** from its residues the Chinese Reminder Theorem (CRT) has to be applied:

$$X = \left(\sum_{p=1,T} xp \ \frac{M}{mp}\ bp\right) mod\ m_1 \quad (4)$$

For each $p \in [1, T]$, b_p is multiplicative inverse of ***M/mp*** **modulo** ***mp*****, that is** $\left(bp\frac{M}{m_1}\right) mod\, m_1 = 1$**.CRT** has the ability to reconstruct integers in a certain range from their residues modulo a set of pairwise relatively prime moduli [14]. Although RRNS could provide representations to all integers in the range *[0, M·MR),* but the legitimate range of representation is limited to *[0, M).* The corresponding (*T+R*)-tuples are called legitimate while integers in *[M, M·MR)* and the corresponding (*T+R*)-tuples are called illegitimate [15].

As described in [5], the RRNS technique can be used to achieve the confidentiality of distributed data as follows: Suppose a file created by u_i. The file is partitioned into a sequence of *n* records where each record consists of *b* bits. Record is encoded in the *RRNS* to produce residues. Residues are distributed to different nodes for storage. Storage nodes, in turn, associates the residue with unique identifier in an available location in its storage, and returns to $u_i$the identifier of the location in the encryption form to enforce confidentiality. The owner $u_i$keeps a file descriptor *F*, containing the moduli and *n record descriptors*; the record descriptor contains the (distinct) nodes storing the residue digits and the identifiers. In order to read (recover) the file the reader must has file descriptor therefore it must share it. To allow node *j* to share a file descriptor *F*, $u_i$encrypt the *F* with public key of *j and send it* to u_j. The reading procedure executed by a node owning the file descriptor *F*. At the beginning, $u_i$sends read requests to nodes storing residues; the parameter of the read request sent is the identifier of the residue. When the node receives a copy of the requested residue, it sends it back to *reader node*. Finally, reconstructing the record involves the execution of the *Chinese Remainder Theorem.* If the owner needs to remove the file, he/she will send a set of messages to all the nodes storing the record residues, requesting deletion of the residues. Also, another set of messages are sent to all nodes sharing the file descriptor requiring from them to discard it.

5. The Proposed System Architecture

Theproposed system aims to achieve confidentiality, dependability, authenticity,and dynamic integrity in the distributed storage system that support creating and sharing files under a write-once mode. Our proposal represents an enhancement and modification of the work proposed in [5] which mainly used to encode files in Redundant Residue Number System (RRNS).The RRNS technique ensures the requirements of confidentiality and dependability [17]. In addition, the RSA algorithm and digital signatures are used to provide authentication, non-repudiation (A sender should not deny having sent and signed a message), and Integrity. It is important to emphasize that there are no actual energy limitations that can prevent using the RSA (or other public key algorithms) in the proposed system. Despite their relatively high computing energy requirements, such public key algorithms are only used in the upper layer of the network hierarchy that includes various system servers. In other words, the RSA is not applied on the lower level of the network that incorporates

sensors with critical energy constraints. The security techniques for achieving integrity and authentication at sensor level is out of scope of this work. The main phases of the proposed system are depicted in Figure 2. These phases are also described in the following subsections.

5.1 RRNS Encoding Phase

A Microsoft Access 2010 database that contains a number of patients records has been built. This database is initially stored in owner server. The PRNS technique is applied on the information of each patient. The *T+R* moduli (keys) are chosen from library of moduli that hasbeen borrowed form [17]. This library was built so as to meet all required specifications of moduli (such as primality, being positive integers, and have generality). Note that *T* and *R* are set by the user (R refers to redundancy). Then data is partitioned into *n* records. Next, we find the residues bytaking each record (in decimal form) and apply equation (2), which can be re-written as follows:

$$residue = record \ \ mod \ modulus \quad (5)$$

The main steps in this phase are shown in Figure 3.

5.2Digital Signing Phase

This phase takes the residues that are required to be sent to different server and applies DSA to sign them. To create a signature, two quantities *r* and *s*are calculated, that depend on the public key components *(p,q,g)*, the owner server's private key (*x*), the hash code of the residues represented as *M* and *H(M)*, and an additional integer *k* that should be generated randomly or pseudo randomly and be unique for each signing process. The following equations represent this process (See also Figure 4).

$$s = f1(H(M), k, x, r, q) = \left(k^{-1}(H(M) + xr)\right) mod\, q \quad \textbf{(6)}$$

$$r = f2(k, p, q, g) = (g^k mod\, p) mod\, q \quad \textbf{(7)}$$

5.3 Distribution of Residues Phase

In this stage, the residues (*s* and *r*) are distributed into *T+R* of trusted servers in order to store them. The process of distributing residues to servers is done arbitrary with the one constraint that different residues of the same record should be stored in different servers.

5.4Signature Verification and Authentication Phase

In this phase, the delivered residues are verified to check that they have not been altered during the transmission. Also, the identity of sender is verified (to ensure the integrity and authentication at the same time). The Verification process is performed as follows: The storage receiver generates a quantity *v* that is a function of the public key components, the owner server's public key, and the hash code of the incoming residues. If this quantity matches the components of the signature, then the signature is validated. The following equations represents these steps (See Also Figure 5).

$$w = f3(s', q) = (s')^{-1} mod\, q \quad \textbf{(8)}$$

$$v = f4(y, q, g, H(M'), w, r') = \left((g^{(H(M')w) mod q} y^{r'w mod q}) mod\, p\right) mod\, q \quad \textbf{(9)}$$

Figure 2. Main phases of the proposed system.

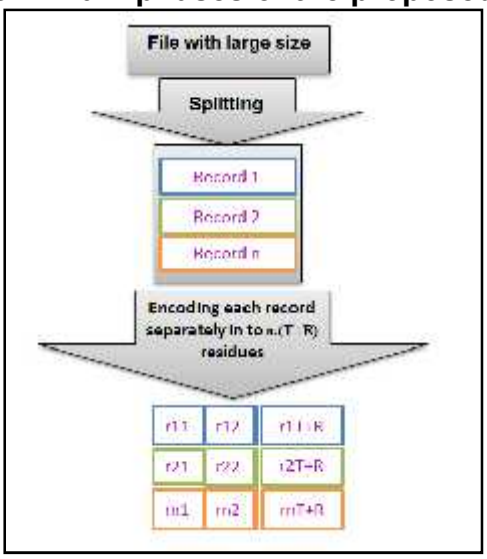

Figure 3. Splitting and encoding steps.

After completing the verification process, the received residues with its identifiers are stored in storage servers in their proper locations. These identifiers must be returned to the owner server. Here the RSA encryptionof the identifiers with the public key of owner server is used for achieving authentication. An owner server creates file descriptor *F* that will be sent to servers that want to reconstruct the patient's information.

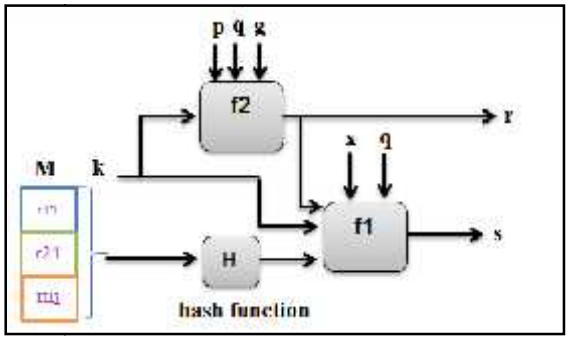

Figure 4. The signing process

5.5 Information Reading Phase

In order to allow to trusted server to read the patient's information, that server must share the file descriptor in a secure manner using the RSA algorithm. After the process of sharing the file descriptor is completed, it is possible to directly proceed to the reading process using similar steps to those described in [5]. Alternatively, it might be desired to significantly enhance the security of this phase by requiring another signing process in the storage server on stored residues. Thus, when the information is sent to the reader server, the reader apply the required verifying process. However, this can increase time and computational overhead. This point still needs some further investigation.

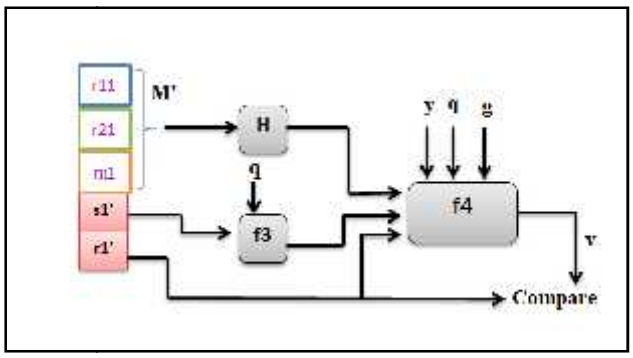

Figure5. The verification process.

6. Conclusion

WBAN have architecture consist of sensors deployed on human body, sending sensing data to medical server that in turn transmits these data to the remote server. Securing this sensitive data is very important in order to keep the security and privacy of patients. This paper focused on methods for distributed storage of this data by surveying recent related work that tried to achieve the requirements of data security. The paper also have introduced asystem proposal that depends on specially combined techniquesof RRNS encoding, public-key cryptography, and digital signatures to achieve confidentiality, dependability, integrity and authentication in the distributed storage system. This paper represents a work-in-progress report of our system that is being implemented using C# language based simulation. More results of this simulation will be described in a subsequent paper.

References

[1] Benoit Latre,BartBraem, Ingrid Moerman, Chris Blondia, andPiet Demeester,"A Survey on Wireless Body Area Networks", 2010.

[2] Ming Li and Wenjing Lou, "Data Security And Wireless Body Area Networks", IEEE Wireless Communications, February 2010.

[3] Chris Otto, AleksandarMilenković, Corey Sanders, Emil Jovanov," System Architecture Of A Wireless Body Area Sensor Network For Ubiquitous Health Monitoring", Journal of Mobile Multimedia, 2006.

[4] Qian Wang and KuiRen, Wenjing Lou, Yanchao Zhang," Dependable and Secure Sensor Data Storage with Dynamic Integrity Assurance",IEEE INFOCOM 2009 proceedings.

[5] Chessa and P. Maestrini,"Dependable and Secure Data Storage and Retrieval in Mobile, Wireless Networks", International Conference on Dependable Systems and Networks, 2003.

[6] Mohammed Raza Kanjee, Kalyani Divi, and Hong Liu," A Two-Tiered Authentication and Encryption Scheme in Secure Healthcare Sensor Networks", Sixth International Conference on Information Assurance and Security, 2010

[7] Sofia NajwaRamliandRabiah Ahmad,"Surveying the Wireless Body Area Network in the realm of Wireless Communication", 2011.

[8] BenoîtLatré," Betrouwbare en energie-efficiëntenetwerkprotocollenvoordraadloze Body Area Networks", 2008.

[9] ShervinAmini, Richard Verhoeven, Johan Lukkien, Shudong Chen,"Toward a Security Model for a Body Sensor Platform", International Conference on Consumer Electronics (ICCE), 2011 IEEE .

[10] Chol-Soon Jang, Deok-Gyu Lee, and Jong-wook Han," A Proposal of Security Framework for Wireless Body Area Network", International Conference on Security Technology, 2008.

[11] Michael O. Rabin," Efficient Dispersal of Information for Security, Load Balancing, and Fault Tolerance",Journal ofthe Association for Computing Machinery. Vol. 36, No. 2, April 1989, pp. 335-348.

[12] ArunSubbiah and Douglas M. Blough," An Approach for Fault Tolerant and Secure Data Storage in Collaborative Work Environments", StorageSS'05, November 11, 2005.

[13] N. Subramanian, C. Yang, and W. Zhang, "Securing distributed data storage and retrieval in sensor networks," in Proc. IEEE PerCom, 2007.

[14]William Stallings, *Cryptography and Network Security Principles and Practice*, Fifth Edition, Prentice Hall, USA, 2011.

[15] Manuel Mogollon,*Cryptography And Security Services: Mechanisms and Applications*, University of Dallas, CyberTech Publishing, USA, 2007

[16]Lie-Liang Yang and LajosHanzo," Coding Theory and Performance Of Redundant Residue Number System Codes", School of Electronics and Computer Science, University of Southampton, SO17 1BJ, UK. [17]S. Chessa, R. Di Pietro, and P. Maestrini," Dependable and Secure Data Storage in Wireless Ad Hoc Networks: An Assessment of DS2", IFIP International Federation for Information Processing, 2004

خصوصية وأمنية البيانات الموزعة في أنظمة الصحة الإلكترونية المتعلقة بشبكات منطقة الجسم اللاسلكية

أ.م.د. سفيان تايه فرج*، م. د. علي جبير داود*،عبيرداودسلمان*

المستخلص

لقد برزت شبكات منطقة الجسم اللاسلكية (WBAN) كتقنية جديده للرعاية الإلكترونية عن طريق جمع البيانات الخاصة بالحركات والمتغيرات الحيوية للمريض عن طريق متحسسات صغيره ممكن ارتداؤها أو زرعها في جسم المريض. وهذه المتحسسات تتصل فيما بينها عن طريق تقنيات الاتصال اللاسلكية ذات المدى الصغير. وقد أظهرت شبكات منطقة الجسم اللاسلكية إمكانيات كبيرة في تحسين نوعية الرعاية الصحية، ولذلك تم استخدامها في تطبيقات واسعة. غير أن توفير الأمنية والخصوصية للبيانات المجمعة من هذه الشبكات أثناء خزنها داخل الشبكة أو نقلها خارجها هو مصدر قلق بحاجة إلى حل مناسب؛ حيث أن هناك تحديات ناتجة عن القيود الصارمة لمصادر أجهزة هذا النوع من الشبكات. إن الهدف الرئيسي من هذا البحث هو تحقيق خزن البيانات الموزعة بشكل مؤمن ومعتمد عليه في مثل هذه الشبكات. وفي الجزء الأول من هذه المقالة سيتم مراجعة أهم ما تم نشره من البحوث السابقة ذات العلاقة بموضوعنا. وسيتم مقارنة آخر التوجهات البحثية في المجال مع بعضها للتعرف على ميزات وسلبيات كل منها. ومن ثم سيتم تقديم مقترحنا على أساس ذلك ، وهو يعتمد بالدرجة الأساس على دمج استخدام تقنيات ترميز المحو، ومشاركة السر، والتوقيع الجبري سوية من اجل تحقيق السرية والاعتمادية وسلامة البيانات.

* كلية الحاسوب ، جامعة الأنبار