Wireless Personal Communications (2022) 122:1767–1806
https://doi.org/10.1007/s11277-021-08969-0

Challenges and Developments in Secure Routing Protocols for Healthcare in WBAN: A Comparative Analysis

Ripty Singla[1] · **Navneet Kaur**[2] · **Deepika Koundal**[3] · **Anuj Bharadwaj**[1]

Accepted: 9 August 2021 / Published online: 22 August 2021

Abstract
The rise in life expectancy of humans, COVID-19 pandemic and growing cost of medical services has brought up huge challenges for the government and healthcare industry. Due to unhealthy lifestyle, there is an increased need for continual health monitoring and diagnosis of diseases. Wireless Body Area Network (WBAN) is attracted attention of researchers as various biosensors can be embedded in or worn on the body of human beings for the measurement of health parameters. The patient's health data is then sent wirelessly to the physician for health analysis. The biosensors used to measure physiological parameters have limited power due to its small size and hence smaller form factor. For the longevity of the network, it is imperative to transmit the data in an energy-efficient manner. Moreover, the health information of the patient is stringently private. Hence, the privacy and security of transmitted information needs to be ensured. It necessitates the development of effective, lightweight and secure routing protocols that provides security with minimal use of resources. This paper has identified the numerous security requirements in WBANs and has provided the extensive review on existing secure routing protocols reported in the literature. A comparative analysis of the various existing state-of-the art secure routing protocols and critical analysis based on security techniques along with different performance parameters has been presented.

Keywords Wireless body area networks · WBAN · Routing protocols · Security · Cryptosystems · Energy efficient

✉ Navneet Kaur
navneetsehgal5@gmail.com

Ripty Singla
ripty.e8896@cumail.in

Deepika Koundal
dkoundal@ddn.upes.ac.in

Anuj Bharadwaj
anuj2k3@gmail.com

[1] Department of Computer Science and Engineering, Chandigarh University, Mohali, India

[2] Department of Computer Science, Chandigarh University, Mohali, Punjab, India

[3] Department of Virtualization, School of Computer Science, University of Petroleum & Energy Studies, Kandholi, Dehradun, Uttarakhand, India

1 Introduction

COVID-19 pandemic, bad lifestyle choices, inadequate relief of chronic stress, rising cost of healthcare services and increasing elderly population presented huge challenges for the government and healthcare industry in developed countries [1, 2]. Millions of people in the world die due to heart diseases, asthma, cancer, diabetes, obesity and many more critical syndromes every year [3]. Need for health care systems and disease management is more than ever [4, 5]. The future healthcare systems should focus on early monitoring and cure of diseases for improvement in the superiority of life [6].

Wireless Body Area Network (WBAN), also known as medical evolutionary application of Wireless Sensor Network (WSN) occurred as a potential technology to provide the state of art quality in the health care systems [7]. In 2001, Van Dam et al. first coined the term WBAN [8]. WBAN is defined by IEEE 802.15.6 as "A communication standard optimized for low power devices for their operation on, in or around the human body (but not limited to humans) to serve a variety of applications including medical, consumer electronics or personal entertainment and other" [9]. In WBAN, various biosensors are embedded in or placed on the human body to collect and analyse the physiological parameters of patients. This medical information is transmitted to a Body Coordinator (BC), either placed on or near the body. The BC further transmits this information to the doctor, health care centre or any other required destination [10]. It has distinct challenges in terms of security, energy efficiency, heterogeneous data generation rate and size, dynamic network topology, stringent Quality of Service (QoS) requirements and low power consumption [11].

The physiological information of the patients is stringently private [12]. The tampering of medical information by any intruder may cause serious concerns for the patients. It may be a matter of life and death of the person [13]. Therefore, communication of physiological information among all sensors in WBAN and its further transmission needs to be secure [14]. The malicious attacker can utilize the obtained information for illegitimate purposes. This necessitates the development of security mechanisms and methods in WBAN to protect the physiological information and privacy of patients. Many routing protocols have been proposed in literature to resolve these issues but as far as the authors best knowledge none of these surveys have categorized the routing protocols on the basis of their cryptographic schemes. This paper presented a comparison and critical analysis of various routing protocols in terms of techniques used, energy efficiency, security and computational overhead. This paper contributed the research in the following manner: (1) A new categorization of WBAN routing protocols based on different cryptosystems has been presented. In each category, detailed discussion of prevailing research on WBAN environment has been carried out to identify pros and cons of each work. (2) Systematic literature review has been performed for most appropriate routing protocols taking into consideration the security of the physiological information by mitigating various security attacks. (3) Systematic evaluation has been performed on each routing protocol to identify various parameters that can enhance the privacy and security of data from different security attacks in WBAN. (4) Critical security analysis has been performed for encouraging better solutions of the existing limitations.

Rest of the paper is structured as: The architecture of WBAN is discussed in Sect. 2. Section 3 shows the organized literature review of different security requisites. Section 4 presents the categorization of existing routing protocols based on their characteristics and nature of cryptographic techniques and focuses on the fact findings and their discussions. Section 5 discusses the conclusion and future scope.

2 WBAN Architecture

Figure 1 illustrates the architecture of WBAN that has been classified into three different tiers.

Tier-1 Intra-WBAN In tier-1, the sensor nodes or biosensors used to communicate with each other having radio transmission range of approximately 2 m. The sensor nodes transmit the measured physiological information to the Body Coordinator (BC). Point-to-point (P2P) links are established among the body sensors for communication between BC and body sensors as well as among the body sensors [16].

Tier-2 Inter-WBANs Tier-2 lies between various Access Points (APs) and BC. Multiple APs can be used to help sensor nodes for further communication. BC or Personal Server (PS) sends the aggregated and processed data to various access points. Inter-WBAN connects WBANs in different networks for easy access on a daily basis. These networks may be Internet or the cellular networks. ZigBee can be used as tier-2 communication technique [17].

Tier-3-Beyond-WBAN This communication tier is between WBAN and outside networks, e.g. internet. BC and APs can directly communicate to the outside network. The design of tier-3 is application-specific. APs aggregate the whole data and further transmit to the physicians or doctors. Thus patients or doctors can be easily informed of an emergency status [18].

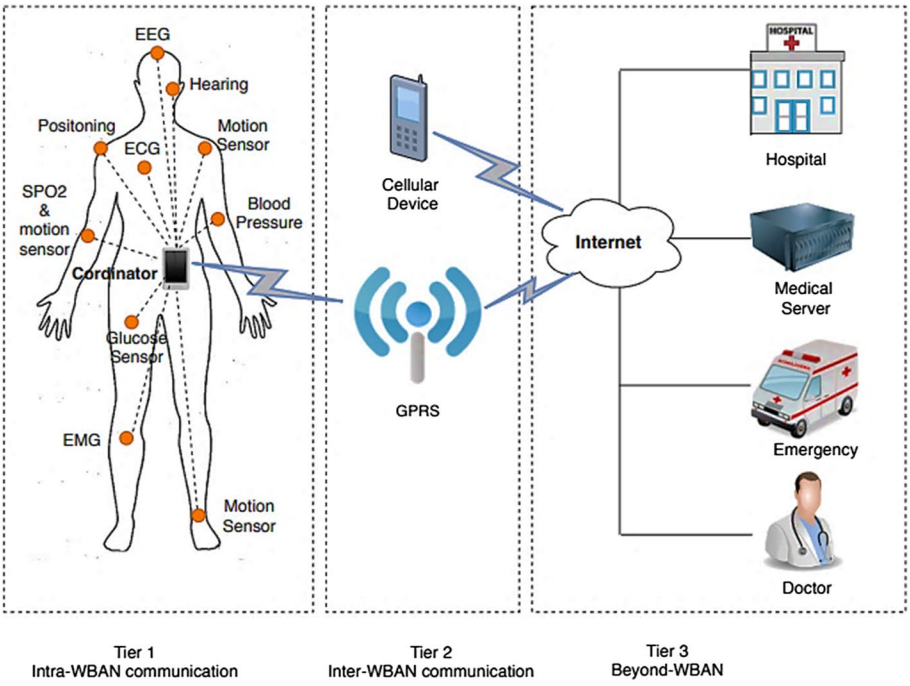

Fig. 1 WBAN Architecture [15]

3 WBAN Security Requirements

Security is an imperative challenge that needs to be addressed. Figure 2 illustrates different types of WBAN security requirements viz. privacy protection, network communication security and data storage security.

3.1 Privacy Protection Requirements

Due to the sensitive and private nature of physiological information, people may have hesitation in accepting WBAN without proper privacy implementations. The privacy protection requirements such as data access control, revocability, data confidentiality, accountability restricts the dissemination and collection of personal information [19].

Data Confidentiality assures that physiological information is not made accessible to illegitimate people. A malicious attacker can observe the communication between sensors and BC. The acquired information can be utilized for illegitimate purposes. To address data confidentiality, various data encryption techniques have been used in WBAN literature [20]. Many researchers have recently contributed to the data confidentiality requirements of WBAN [21–27]. Data Access Control provides role based access of the private information of patients to doctors, physicians or any other parties where it is needed. In case, an insurance agent happens to access patient's health information then patient may be discriminated in giving insurance at a high premium [28]. To resolve this, different techniques

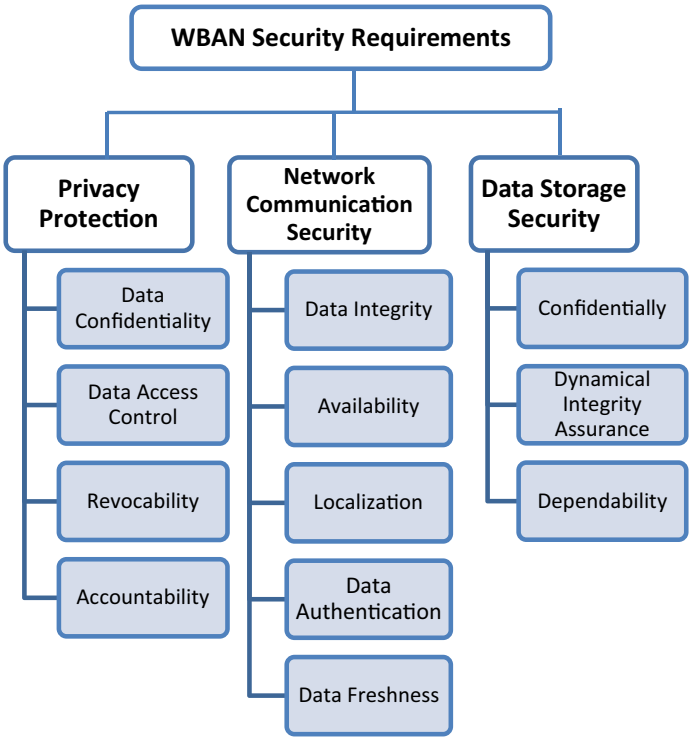

Fig. 2 WBAN security requirements

are used in WBAN literature such as Medium Access Control protocols (MAC protocols), role based access control etc. [29–35]. Revocability assures when a user/node is identified as malicious in the system then all previously granted permissions needs to be revoked from it to make the rest of the system secure [20]. Joshi et al. [27] introduced the light-weight authentication routing protocol to efficiently provide revocation based on Elliptic-Curve Cryptography (ECC) with reduction of the complexity at client-side. Accountability is an essential service to implement data access control in WBANs. In general, two reasons are responsible for data breach. First, when a legitimate user carries unauthorized activities on patient 's information i.e. misuses his privileges. Second is data mishandling i.e. sensitive information is stolen or used by an illegitimate user. In both cases, that user should be recognized and held accountable [36].

3.2 Network Communication Security Requirements

The physiological information is transmitted across different networks for further communication in different tiers of WBAN. Therefore, network communication security requirements viz. data integrity, availability, localization, data authentication, data freshness are necessary to be implemented. Data Integrity assures that patient's information is not being altered by a malicious attacker. The modified information can lead to wrong treatment of patient and may have terrible consequences [37]. To ensure accuracy and integrity of the received information, different techniques are used in WBAN literature such as Message Authentication Code (MAC), hash functions and digital signatures [38–41]. Availability assures that the required information remain accessible 24*7 to the doctor even after Denial-of-Service (DoS) attack [42]. Suppose if an attacker disables the ECG (electrocardiogram) sensor of a heart disease patient; this would lead the patient into critical situation or even death [38]. The WBAN literature has suggested various ways to cope up with DoS attack [43–48]. Localization service finds the location of biosensors in a dynamic network. Each bio-sensor should be capable to locate its own position. Absence of localization may allow an intruder to transmit wrong location of the patient [38]. Many researchers have recently contributed to the localization requirements of WBAN [49–52]. Data Authentication is desirable in both medicinal and non-medicinal areas. Absence of data authentication may allow an illegitimate person masquerades as legitimate user. The illegitimate person may provide wrong patient data to the BC. This can create a situation where false instructions are given to the body sensors/actuators which may cause harm to the patient [53]. To address data authenticity in WBAN, various cryptosystems, biometrics, MACs are used [54–61]. Data Freshness assures that the received data frames are in order and no malicious attacker replayed old messages. Two categories of data freshness are considered: (a) weak freshness and (b) strong freshness [62]. Weak freshness is limited to the accurate ordering of data frames but without consideration of delay parameter. Accurate ordering as well as delay in data frames constitutes strong freshness. Both types have their own significance in WBAN. Weak freshness is needed by low-duty cycle body sensors like blood pressure and strong freshness is for synchronization [63]. Many researchers have proposed useful solutions for this service in WBAN scenario [64, 65].

3.3 Data Storage Security Requirements

Along with data transmission, security is also important for sites where data is stored [66]. The various data storage security requirements in WBAN are confidentially, dynamical

integrity assurance and dependability. Data Confidentially is essential not only during transmission but also during storage. The sites where data is stored must be secured in order to keep patient's information confidential to prevent getting misused. Dynamical Integrity Assurance dynamically checks and finds alteration in stored data in the storage space of entities present in the network before transmission of the data. Consider a situation where a sensor node fails due to energy constraints or some malicious modifications. To retrieve information readily from such nodes, dependability service should be considered [67]. It has received limited attention although it finds great importance in WBANs.

4 Classification of Secure Routing Protocols for WBAN

The routing protocols act a substantial role for the efficient communication in WBAN. Routing is defined as the process of choosing the best route among the available routes in order to send the packets at their destination efficiently. Security issues and challenges of WBAN have motivated the researchers to propose secure routing protocols. The taxonomy of existing secure routing protocols in WBANs is shown in Fig. 3.

4.1 Symmetric Key Cryptographic Protocols

Symmetric key cryptographic routing schemes provide security solutions for the various security threats in WBAN using a shared secret key for both encryption and decryption. These protocols are efficient, take less time for encryption/decryption process and have low overhead and communication cost [68]. The following sections discuss various symmetric key cryptographic routing protocols for WBANs.

4.1.1 Advanced Encryption Standard (AES) Encryption Framework

The AES framework [69] provides the usability of AES and its modes for WBAN to improve security in accordance with WBAN data traffic categorized as on-demand data, emergency data, and normal data. Different security modes of AES are Cipher-Block Chaining-Medium Access Control (CBC-MAC), Counter (CTR), and Counter with CBC-MAC (CCM). Each security mode of AES has usage based on the security requirements of an application and selected using an Access Control List (ACL).

The CTR mode is used to encrypt the data of sensor nodes to achieve confidentiality. First, the plaintext is divided into blocks $b_1, b_2, b_3 \cdots \cdots b_n$ each having a size of 16 bytes. Then encryption and decryption process of CTR mode is applied as represented in Eq. (1) and Eq. (2).

$$\text{For Encryption } c_i = b_i \oplus E_k(x_i) \tag{1}$$

$$\text{For Decryption } b_i = c_i \oplus E_k(x_i) \tag{2}$$

where b_i is block of plaintext, $\oplus$ is XOR, c_i is the ciphertext obtained after encryption and $E_k(x_i)$ is the encrypted counter x_i. The overall working of CTR mode is illustrated in Fig. 4.

In addition to confidentiality and authentication, data integrity is also important. CBC-MAC mode of this framework helped in achieving data integrity. To achieve the final ciphertext, previous ciphertext blocks are XORed with the plaintext blocks.

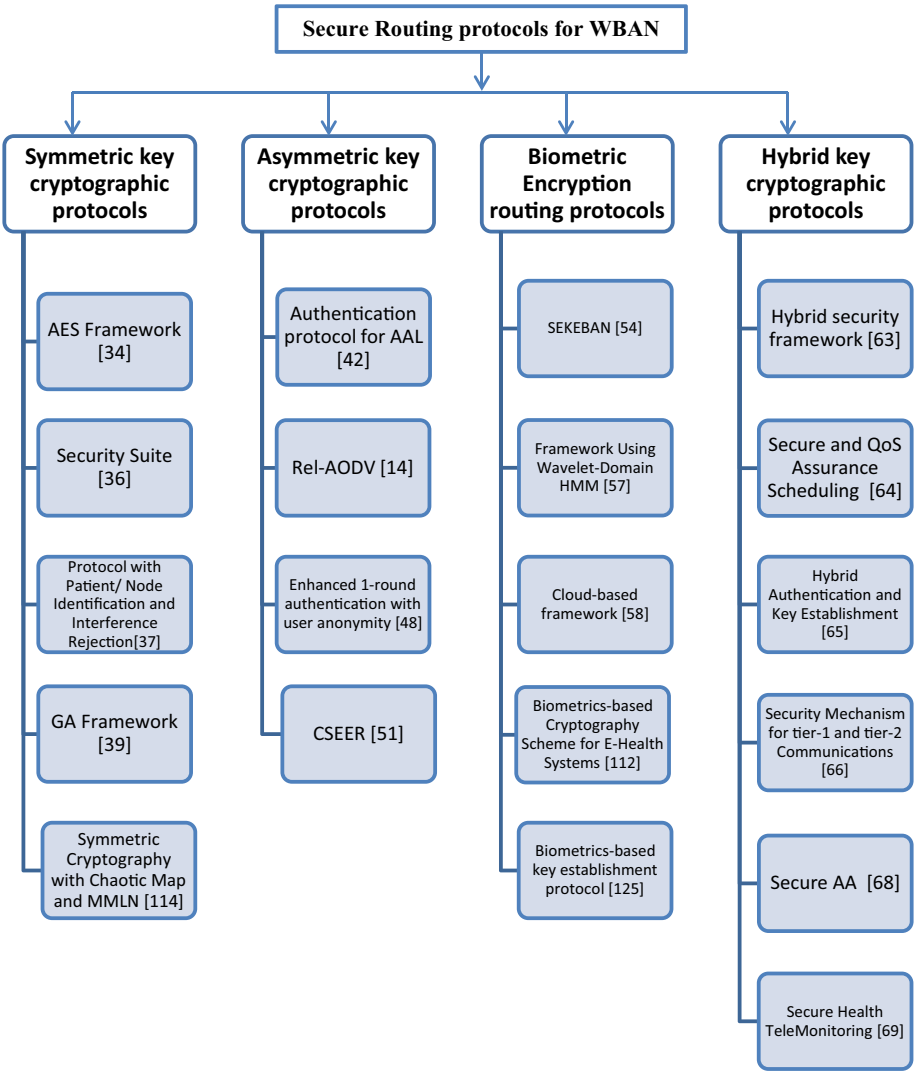

Fig. 3 Classification of routing protocols based on different cryptosystems

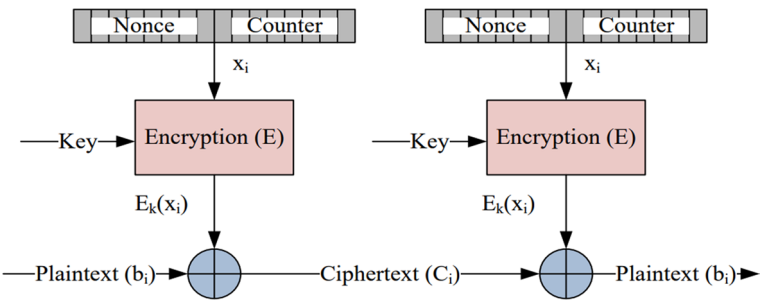

Fig. 4 CTR mode [69]

Equation (3) and Eq. (4) represents the mathematical representation of encryption and decryption process. The overall working of CBC-MAC mode is illustrated in Fig. 5.

$$\text{For Encryption } c_i = E_k\left(b_i \oplus c_{i-1}\right) \tag{3}$$

$$\text{For Decryption } b_i = D_k\left(c_i \oplus c_{i-1}\right) \tag{4}$$

where, b_i is block of plaintext,c_i is the ciphertext, $\oplus$ is XOR and E_k is the encryption of $\left(b_i \oplus c_{i-1}\right)$, D_k is the decryption of $(c_i \oplus c_{i-1})$ and c_{i-1} is previous block of ciphertext.

To assure high-level security including both confidentiality and data integrity, AES-CCM mode incorporated both the CTR and CBC modes. Integrity protection is achieved using CBC-MAC mode and confidentiality using CTR mode. Thus, AES-CCM mode is preferred for transmitting life-critical information. Law et al. [70] established the best energy efficient encryption/decryption process as AES. The authors also supported the use of stream cipher for encryption as it is convenient to use due to same size of the plaintext and the ciphertext.

4.1.2 Security Suite for WBAN

WBANs become vulnerable if keys used in cryptographic algorithms are compromised. This can happen during key exchange phase of security mechanisms for communication in the network. The removal of this phase is necessary because if the initial phase is compromised then the whole system becomes vulnerable. Sampangi et al. [71] presented a security suite comprising of Key Management and Encryption for Securing Inter-Sensor Communication (KEMESIS) and Independent and Adaptive Management of Keys (IAMKeys) scheme that eliminated the need for exchange of keys. KEMESIS is a key management system to secure inter-WBAN communication. IAMKeys is an adaptive and independent key management system for increasing the security of WBANs. These schemes independently generated a random key for encrypting data frames at both communicating ends and eliminated the need for key exchange in the network. Figure 6 illustrates the security suite.

This scheme also provides the optimization of resource utilization by excluding the requirement for an isolated authentication process using digital signatures. To analyse the security, various attacks viz. session hijacking, Man-In-The-Middle (MITM) and replay attack have been considered. This security suite has found the balance between optimal resource utilization and security. This scheme is a basic attempt for optimal operation of WBANs. It reduces the total computational overhead but has varying complexity and reliance on human for randomness of initial data frames.

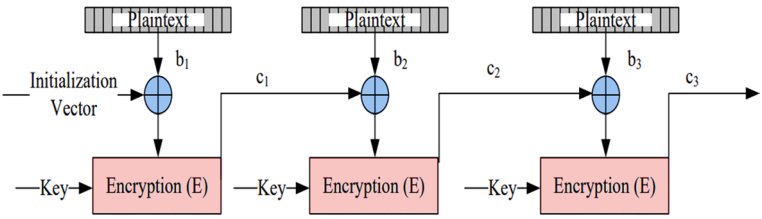

Fig. 5 CBC-MAC mode [69]

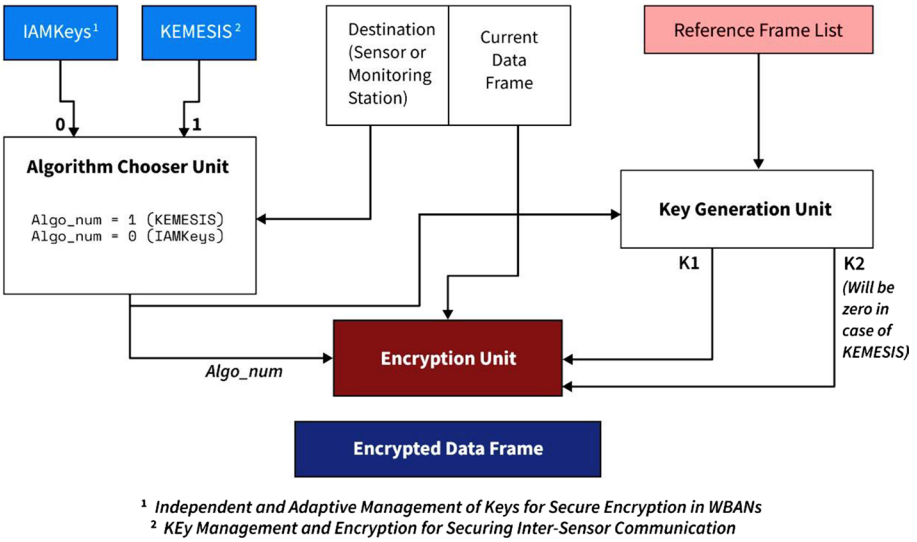

Fig. 6 Security suite [71]

4.1.3 Protocol with Patient/Node Identification and Interference Rejection

Baqai et al. [72] presented a routing protocol which provides the secure transmission and is energy efficient in WBAN. It helps in identification of patients/nodes, provides inherent security and rejects interference from Infrared (IR) sources and false data invaders. Low energy consumption is on account of two reasons. First, no extra encryption hardware is required. Second, the sensors can sleep in time slots when no transmission is taking place in the system. Sensor nodes are linked with the Base Station (BS) using star topology. This protocol is implemented in a cost effective manner using IR transceiver and Arduino Microcontroller. The conceptual diagram of this protocol is described in Fig. 7 and its design and implementation is presented in [73]. The results have shown high accuracy of this protocol over short ranges.

4.1.4 Genetic Algorithm (GA) Framework in WBAN

Kumar and Sharma [74] used GA to generate rules for the protection of data storage and transmission as well as to build more random, complex and unpredictable shared key for data security in WBAN. The block diagram for GA in WBANs is shown in Fig. 8. AES is used for encryption of patient data because of high calculation speed and low overhead in key management. To generate key, any image such as ECG sensor image or biometrics or sound frequency of patient or any sensation of body can be considered. An image can be treated as an element of two components: (i) $f(x, y)$, where x and y are the spatial directions (ii) the intensity value evaluated as the estimation of the function at certain pair of coordinates (x, y). An image will be considered as two dimensional array and any row can be used as key for cryptography. For speedy results, the optimal population limits can be determined. To increase the population, two images can be used as a single key for cryptography. Fitness function is computed as converting first row of two dimensional array

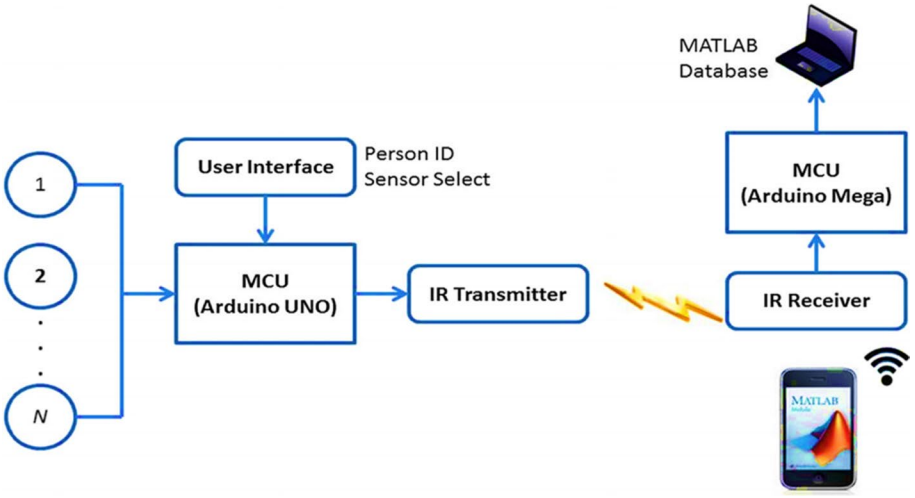

Fig. 7 Conceptual diagram [72]

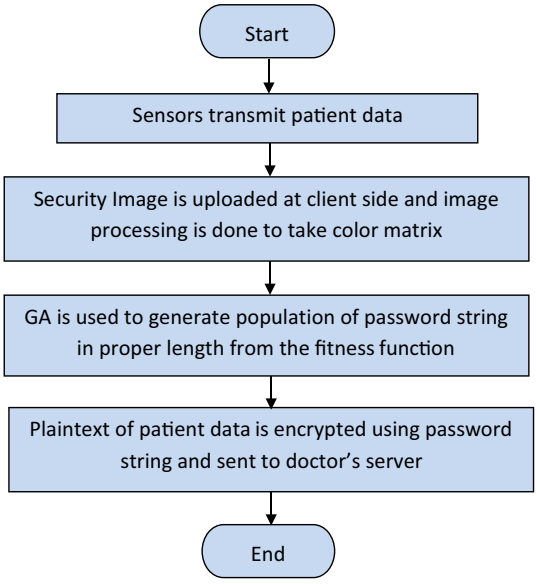

Fig. 8 Block diagram for GA in WBANs [74]

into a decimal number. Size of this decimal number is reduced by any optimality factor such as division by hundred so that its conversion back to binary becomes easy and can be used as population for cryptographic keys. This population is further divided into two halves.

Crossover and mutation operations are performed two times to develop more random and complex key. This key becomes most efficient symmetric key in AES encryption algorithms. In this, the authors provided a framework of hereditary calculation based cryptography and showed a different way for information security in WBANs.

4.1.5 Symmetric Cryptography with Chaotic Map and MMLN

To provide security to ECG signals, Lin et al. [75] proposed a Multilayer Machine Learning Network (MMLN) and chaotic map that updates the network weights using back-propagation algorithm in Multilayer Perceptron Neural Network (MPNN). The authors identified that symmetric cryptographic protocols are prone to active and passive hacker attacks. To overcome passive attacks, chaotic map-based systems are preferred due to generation of random and non-periodic shared secret key [76–80]. The ECG signal is first converted digitally in the range of 0 to 255 and these values are permutated at random by chaotic secret keys. A General Regression Neural Network (GRNN) based model [81–84] has used the training patterns of input–output pairs for constituting the design of MMLN. To ensure the periodic updating of secret key, GRNN-based models used the Particle Swarm Optimization (PSO) algorithm for adjusting the network parameters and determining the global minimum which is further trained for cryptographic procedure [81–83, 85]. This model overcame the flaws of symmetric key cryptographic methods with fixed secret keys and has quick learning time. The results have shown that decrypted ECG signals are reliable, good in quality and obtained without any attacks and noise having a mean Peak Signal-to-Noise Ratio (PSNR) $\geq$ 30 dB. Higher the PSNR value, smaller the loss in recovery of decryption of signal. This proposed solution turned out to be feasible as the mean CPU execution time for cryptographic process was very low and uses less computational resources than Chaotic Synchronization Cryptographic System (CSCS).

4.1.6 Comparative Study of Symmetric Key Cryptographic Protocols: Findings and Discussions

Based on the literature review, Table 1 presents the state-of-the art comparison of different symmetric key cryptographic protocols for WBANs in terms of their goal, technique, pros, cons and other characteristics.

The AES framework [69] provided secure communication for WBAN by categorizing the data traffic as per the security requirements of an application. The major challenge was to use different modes of AES to meet different security requirements in the wake of limited power capacity of biosensors. This framework performed well in terms of computational overhead and energy efficiency but failed when initial key exchange phase compromises. The authors of [71] took initial key exchange phase as one of the major challenge along with sender authentication and data freshness for their research. It resulted in better performance than [69] but at the cost of increased computational overhead. Moreover, complexity increased and varied with the number of operations used in hash function. Baqai et al. [72] reported few more challenges like authentication and sensor identification, energy efficiency, packet transmission and reception with rejection of interference. This protocol provided a cost effective solution with low computational and storage overhead. The major challenge in [74] is security optimization through key management. This framework allowed the complex and random key generations in AES without giving any consideration to the energy consumption parameter, thus ignoring one of the key constraints of WBAN. The key challenge for [75] is to secure ECG signal with the usage of GRNN and MPNN by keeping high PSNR.

Comparison of various symmetric key cryptographic protocols in terms of initial key exchange phase, security, energy efficiency and computational overhead has led to the

Table 1 Symmetric key cryptographic protocols

Author	Saleem et al. [69]	Sampangi et al. [71]	Baqai et al. [72]	Kumar and Sharma [74]	Lin et al. [75]
Name of protocol	AES Encryption Framework	Security Suite for WBAN	Protocol with Patient/Node Identification and Interference Rejection	GA Framework in WBAN	Symmetric Cryptography with Chaotic Map and MMLN
Year	2009	2012	2017	2018	2021
Goal	To provide security solutions to WBAN in accordance with data traffic	To design a robust key generation and management scheme	To design a secure protocol with energy efficiency and interference rejection	To generate rules for protection of data storage and transmission for achieving data security	To design a secure routing protocol for physiological signals
Technique Used	AES and its modes	IAMkeys, KEMESIS	Sony protocol [86]	AES and GA optimization	GRNN, MPNN, PSO, MMLN and a chaotic map
Security	Low	High	High	High	High
Initial key exchange phase	Yes	No	No	No	No
Energy efficiency	High	Medium	High	NA	Not considered
Computational overhead	Low	Medium	Low	Low	Low
Pros	Selects security mode using ACL	Random key generation for each frame	Interference rejection from sources	Unique as GA is used in data security for WBAN	High mean PSNR value
	Usage of stream cipher	Transmission of new frame with latest values instead of retransmission	Capable of giving indications in abnormalities	Security optimization through key management using GA	Low mean executing time
	Low network overhead	Independent key generation at both communication entities	Patient/node identification	Biometrics or any image can be used for key generation	Fast operation time in learning
		Prioritize data freshness	Fast computations	Sound frequency or any sensation of body can be used for key generation	PSO algorithm rapidly adjusts the network parameters
		Elimination of key exchange phase	Low storage overhead		Highly Secure
		Ensures sender authentication			No noise interference

Table 1 (continued)

Author	Saleem et al. [69]	Sampangi et al. [71]	Baqai et al. [72]	Kumar and Sharma [74]	Lin et al. [75]
Cons	If initial key compromised, whole network becomes insecure	The lost data frames should be at least 10 for retransmission	Does not consider non line-of-sight communication	Contribution of GA and AES on energy consumption of the network was not studied	Energy efficiency parameter is not considered
	Does not meet stringent security requirements	Rely on humans for randomness of initial data frames	No modulation scheme is considered to improve the performance		
		Varying complexity		Parameters such as throughput, packet dropping rate and packet delivery ratio were not taken into account	GRNN training with the PSO algorithm is done with fixed learning parameters

following conclusions. In terms of security, [69, 72, 74] and [75] have shown better performance as compared to [69]. In terms of eenergy efficiency, [69] and [72] have shown better performance in comparison to [71]. In contrast, [74] and [75] did not considered the energy consumption parameter. For computational overhead, [69, 72, 74] have performed better in comparison to [71] and [75]. Emphasis on data freshness parameter is considered only in [71]. WBANs become vulnerable when initial phase of key exchange used in cryptographic algorithms gets compromised. Elimination of this phase became necessary for enhancing security in symmetric key cryptographic protocols which has been considered by [71, 72, 74] and [75]. Complexity is considered constant for all symmetric key cryptographic protocols except for [71]. Interference rejection from sources has been done only in [72].

4.2 Asymmetric Key Cryptographic Protocols

As WBANs become vulnerable if keys used in cryptographic algorithms are compromised, therefore it is imperative that different keys are used at both communicating ends for encryption/decryption processes.

Asymmetric key cryptographic protocols achieve the same as no key exchange mechanism is followed. Moreover, data is authenticated using digital signatures. Implementation of these protocols is a challenging task because of more overhead and communication cost than symmetric key cryptographic protocols [87]. Also, the data transmission time is more which does not suits the real time traffic of WBAN. Some of these asymmetric key cryptographic routing protocols are discussed below.

4.2.1 Authentication Protocol for an Ambient Assisted Living (AAL) System

AAL systems offer telehealth services. As data is transmitted through open channels, the system becomes vulnerable to various security attacks. Therefore, it is vital to build a secure and robust authentication protocols that can endure several attacks. He and Zeadally [88] presented an effective authentication protocol for encountering different security requirements of the AAL systems. The authors discussed the system architecture of AAL system and reviewed the related authentication protocols (Liu et al.'s protocol [89] and Zhao et al.'s protocol [90]) for their pros and cons. This authentication protocol used ECC; Identification based Public Key Cryptography (PKC) and modified procedure for generation of private key of user which was not considered earlier. This authentication protocol has three entities: (1) the AAL server (2) a controller for the WBAN (3) an end-user. Figure 9 shows the authentication procedure between the user and the controller of WBAN. The earlier research hosted a verification table for authentication purposes which was prone to different security attacks. Since authors of [88] used AAL server that did not maintain this table, it met the security requirements for AAL system and withstands various attacks. The experimental results have shown that this authentication protocol is 5.7 times better than Liu et al.'s protocol [89] and 1.5 times better than Zhao et al.'s protocol [90] in terms of execution time.

4.2.2 Reliable Adhoc On-Demand Distance Vector (RelAODV) Protocol

For the improvement of the reliability of Adhoc On-Demand Distance Vector (AODV) [91], Raja and Kiruthika [14] have introduced a Reliable AODV (RelAODV) protocol,

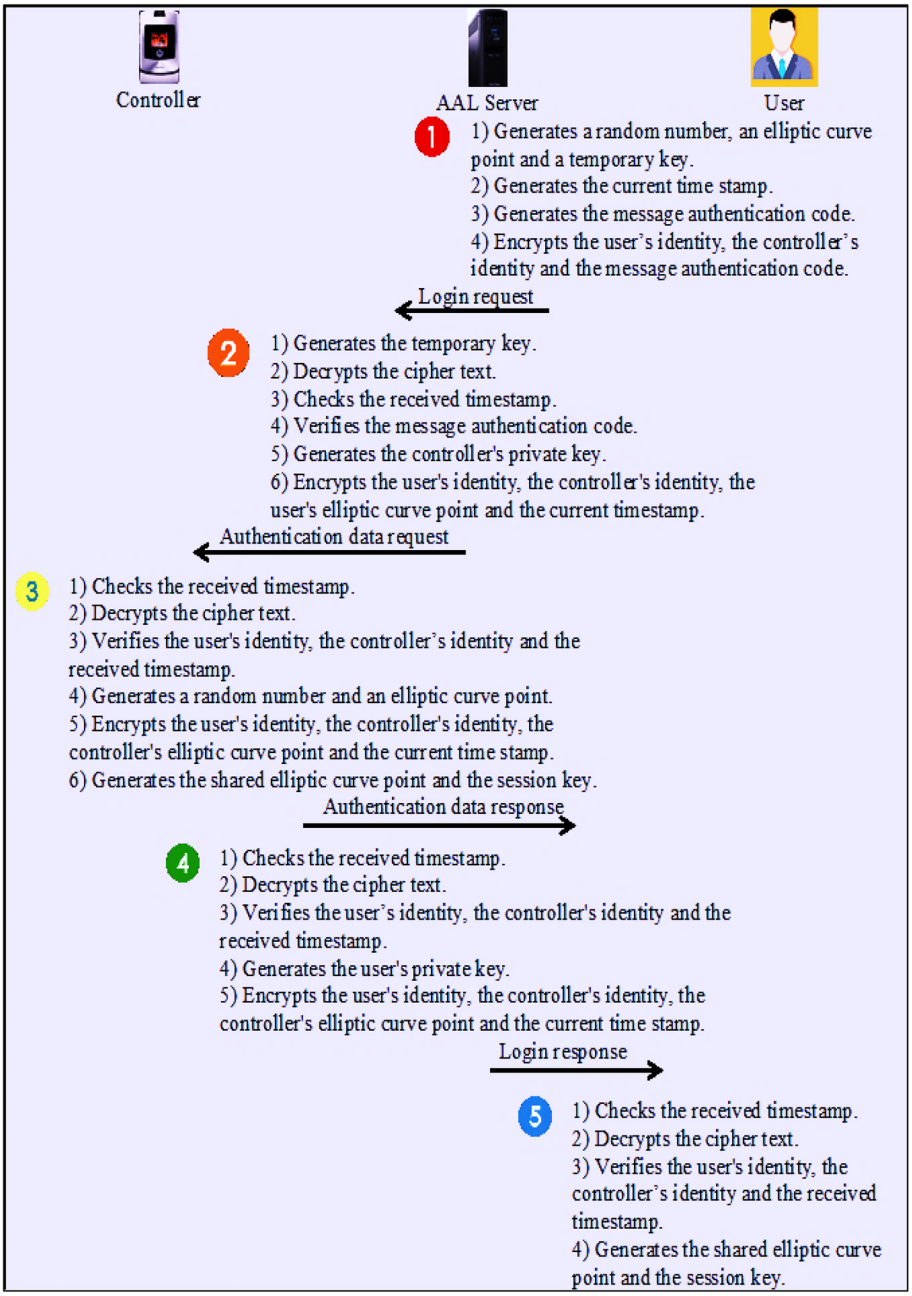

Fig. 9 Process of authentication between the controller and user [88]

also named as Secure and Reliable Data Transmission (SRDT) for the transmission of patient data in an energy efficient way. In this, the biosensors are classified into direct and relay modes to achieve energy efficiency. Rivest, Shamir, Adleman (RSA) cryptographic

algorithm is considered for providing security, privacy and authenticity to the patient data in all tiers of WBAN. Random number generator and nonce database is used to resist replay attack and achieve data freshness.

SHA-1 (Secure Hash Algorithm 1) is utilized for authentication in tier-2 and tier-3 only. SHA-1 was not used for authentication of tier-1 as it increases computational overhead and affects the energy efficiency of tier-1. Rel-AODV [14] protocol is compared with Energy aware Peering Routing (EPR) [15], Co-operative Adhoc On-Demand Distance Vector (C-AODV) [92] and AODV [91] in terms of energy efficiency, throughput, and packets dropping rate. The experimental results demonstrated that Rel-AODV protocol has achieved more energy savings and throughput along with the integration of security mechanisms.

4.2.3 Enhanced 1-Round Authentication Protocol with User Anonymity

Li et al. [93] reviewed 1-round WBAN authentication protocol reported by Liu et al.'s [94] and detected several security flaws such as DoS attack, Key-Compromise Impersonation attack (KCI) and guessing session key attacks. To fix the loopholes, Li et al. [93] introduced an enhanced 1-round lightweight authentication protocol for WBAN with wearable devices. This protocol presented the adversarial model with three entities namely WBAN User/patient (U_i), Network Manager (NM) and Application Server (AS). This protocol consisted of initialization of public and private keys to users, registration of user with NM and authentication phase of users with AS. General process of authentication of this approach is described in Fig. 10. The authors have shown the comparative analysis of this protocol with Liu et al. [89], Liu et al. [94] and Xiong et al. [95] in terms of computational cost and security features. The results demonstrated that this enhanced protocol attained additional security features using formal and informal security analysis but with same cost as Liu et al.'s [94] protocol.

4.2.4 Compressed and Secure Energy Efficient Routing (CSEER) Protocol

For energy saving and high security, Singla and Kaur [96] have presented CSEER Protocol for WBAN. CSEER protocol introduced a multi-objective cost function for the selection of best next hop node on the basis of amount of residual energy and delay for packet transmission in the network. CSEER protocol utilized the two techniques namely, Arithmetic Data Compression technique and RSA algorithm. Arithmetic Data Compression

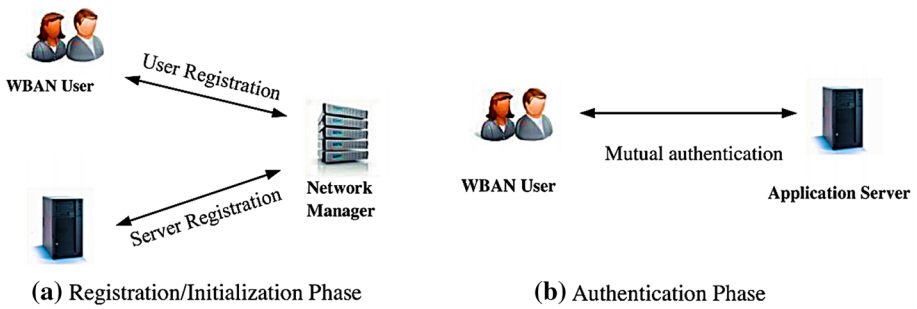

Fig. 10 Authentication process for WBAN [93]

technique compressed the medical data at each node to reduce the size of data as well as to add a layer of encryption for secure data transmissions. RSA algorithm provided high level secure encryption to the patient data. CSEER protocol was compared with EPR [15], Rel-AODV (SRDT) [14] and other conventional protocols [46, 47] in terms of energy efficiency, throughput and packets dropping rate. The experimental results demonstrated that CSEER protocol achieved 11% more energy savings and 3% more throughput than Rel-AODV [14] besides providing security for medical data transmission.

4.2.5 Comparative Study of Asymmetric Key Cryptographic Protocols: Findings and Discussions

All asymmetric key cryptographic protocols intended to eliminate the initial phase of key exchange used in symmetric key cryptographic protocols. A comparison in terms of goal, technique, pros, cons and other characteristics such as energy efficiency, computational overhead and security with other protocols is presented in Table 2.

The AAL systems are vulnerable to security attacks. The major challenge for [88] was to design an Authentication Protocol that could mitigate all security attacks. It performed better than [89] and [90] in terms of computational cost and execution time. The main challenge in [93] was to design an enhanced 1-round lightweight authentication protocol for WBAN by fixing the loopholes given in [94]. As compared to [89, 94] and [95], it showed superior performance in terms of computational cost and security features. The main disadvantage of both [88] and [93] is that these did not consider the significant constraints of WBAN. Compared to EPR [15], C-AODV [92] and AODV [91], Rel-AODV have shown better performance in terms of reliability, throughput, energy efficiency and security but overall routing overhead increased with the transmission of Route Error (RERR) packets during mode switching of sensor nodes. CSEER [96] has performed better than Rel-AODV [14], EPR [15], C-AODV [92] and AODV [91] in terms of energy efficiency, throughput and packet dropping rate with respect to transmission power but did not withstand the replay attack. CSEER [96] is more secure than EPR [15], C-AODV [92] and AODV [91].

By comparing the asymmetric key cryptographic protocols in terms of energy efficiency, data freshness, security and computational overhead, the following conclusions are drawn. RelAODV [14] outperformed in terms of security than CSEER [96]. He and Zeadally [88] and Li et al. [93] have performed better in the implementation of perfect forward secrecy when compared with RelAODV [14] and CSEER [96]. CSEER [96] achieved the better throughput and energy efficiency than RelAODV [14]. On the other hand, both He and Zeadally [88] and Li et al. [93] did not consider the important parameters like throughput and energy efficiency. In terms of computational cost, Li et al. [93] is better than [88] and CSEER [96] is better than RelAODV [14].

4.3 Biometric Encryption Routing Protocols

The biometric signals are random time varying signals and provide high security in key generation [97]. Biometric cryptography refers to an authentication system that combines inherent factors such as ECG, DNA, fingerprints, Iris and other biometric signals with Public-Key Infrastructure (PKI) to enhance the security for WBAN [98]. The following section presents the overview of various biometric encryption routing protocols.

Table 2 Asymmetric key cryptographic protocols

Author	He and Zeadly [88]	Raja and Kiruthika [14]	Li et al. [93]	Singla and Kaur [96]
Name of protocol	Authentication protocol for AAL	Rel-AODV	Enhanced 1-round authentication protocol with user anonymity	CSEER
Year	2015	2015	2017	2018
Goal	To develop a secure and robust authentication protocol for AAL systems	To improve the reliability of AODV protocol	To design secure and lightweight authentication protocol	To achieve energy efficiency and security for medical data transmission
Technique Used	Identity based PKC, ECC, Hash Function	RSA, SHA-1	ECC, SHA-1	Arithmetic Compression, RSA
Security	High	High	High	Medium
Results compared with other protocols	Liu et al.'s protocol [89], Zhao's protocol [90]	EPR [15], C-AODV [92] and AODV [91]	Liu et al. [89] and Liu et al. [94] and Xiong et al. [95]	EPR [15], Rel-AODV [14], C-AODV [92] and AODV [91]
Provides strong forward secrecy	Yes	No	Yes	No
Data freshness	Yes	Yes	Yes	No
Energy efficiency	NA	Medium	NA	High
Computational overhead	NA	High	NA	Medium
Pros	More Efficient than [89] and [90]	Provides reliability	Fixes loopholes of Liu et al. protocol [93]	10–11% more energy savings than Rel-AODV [14]
	Usage of timestamp protocol to resist replay attack	Categorizes traffic of WBAN	Resists to various security attacks	Low congestion in network
	Satisfies all security requirements	High throughput (80%)	More secure than [89, 94] and [95]	High throughput (83%)
	Low execution time than [89] and [90]	Satisfies all security requirements	Same cost as Liu et al. protocol [93]	Reduces the number of bits to be transmitted in Network
	No verification table required	Classification of nodes for energy savings		Low packet dropping rate with increase in transmission power
	Robust and mitigate various security attacks			

Table 2 (continued)

Author	He and Zeadly [88]	Raja and Kiruthika [14]	Li et al. [93]	Singla and Kaur [96]
Cons	Energy consumption of the network is not presented	High routing overhead	Energy consumption of the network is not presented	Path loss parameter is not considered
	Parameters such as throughput, computational overhead not considered	Path loss parameter is not considered	Parameters such as throughput, computational overhead not considered	Data freshness is not considered
				Does not withstand with replay attack

4.3.1 Secure and Efficient Key Exchange for Wireless BAN (SEKEBAN) Protocol

Random time varying signals are having high security in key generation phase [97]. ECG is a random time-varying signal that changes with various physiological activities. Mana et al. [99] presented a methodology that used the physiological features of body such as ECG for addressing the security issues in WBAN. For securing end to end transmission between BC and sensor nodes, an efficient and secure key exchange method called SEKEBAN has been introduced. This method developed and distributed the shared symmetric keys in WBAN and provided the solution for secure communication using biometric data in WBAN. In this protocol, there is an assumption that both BC and the back-end server uses shared symmetric cryptographic session key for securing communication. The session key can be introduced physically during manufacturing or established up by means of symmetric key establishment methods. Another assumption is that all sensor nodes contain Unique device Identifier (UId). The UIds are known to sensor nodes only and manually programmed into the BC.

The UId is never exchanged in plaintext and acts as a primary shared secret between sensor nodes and the BC. The key is generated from random time varying ECG signals. Figure 11 depicts the key generation scheme. Handshake protocol is utilized for initiating the communication between sensor nodes and BC in SEKEBAN. It is used for secure and efficient establishment of symmetric session keys between the communicating nodes in the network. The results demonstrated that it is more energy efficient than SSL protocol [100] and Kerberos protocol [101].

4.3.2 Framework Using Wavelet-Domain HMM

Wang et al. [102] introduced a security model for WBAN that uses various biometric signals of patient to secure data communication among body sensors. A wavelet-domain Hidden Markov Model (HMM) time-efficient classification technique is used to authenticate messages with high accuracy by using ECG signals. Due to high randomness and uniqueness, ECG signal is preferred as the biometric key for the confidentiality and authentication purpose in this framework. Figure 12 represents the biometric-based Security System using HMM. The above given approach consisted of two methods: (1) a HMM-based time-efficient authentication method and (2) an encryption technique using ECG as a shared secret key. The encryption overhead is described with the unit-block encryption time, the number of bits selected for encryption and the encryption block size. In this approach, the selective encryption is used to encrypt only the main modules of physiological information instead of whole available biomedical information. The selective encryption minimized the computational overhead as compared to traditional full encryption methods. Thus, it satisfied the resource constraint issue of WBAN. However, this approach is not limited to only ECG signals. Numerous biometrics can be smoothly and easily integrated into this scheme. The experimental results revealed that this scheme achieved the authentication performance

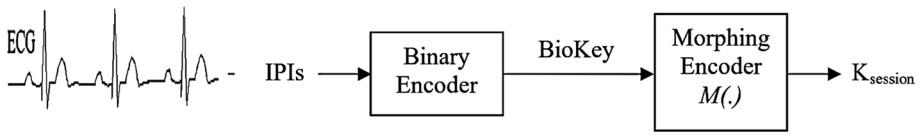

Fig. 11 Key generation from ECG-signal [99]

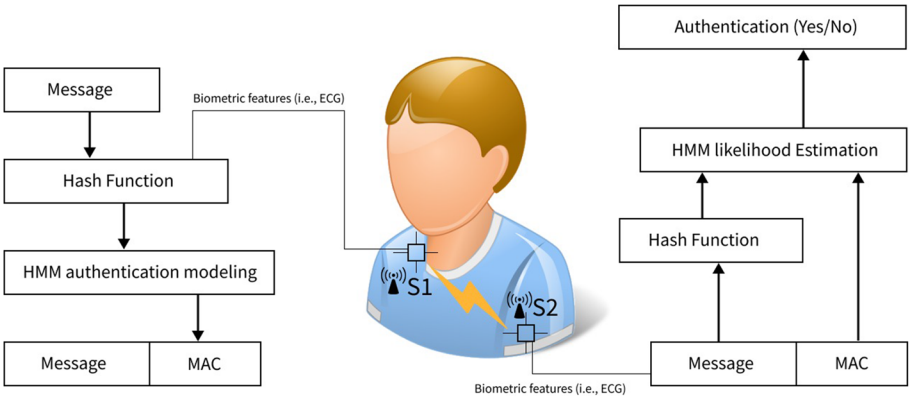

Fig. 12 Biometric-based security system using HMM [102]

with high accuracy without any extra key distribution needs and satisfied the stringent time synchronization.

4.3.3 Cloud-Based Framework

Khan et al. [103] introduced a cloud-based framework for mobile healthcare system because cloud-based applications are most secure. This system emphasized on secure intra WBAN communication and security of patient data. This cloud-based framework is depicted in Fig. 13 and consisted of (i) biosensors embedded in or wearable by patient, (ii) a client interface.

(iii) personal server (iv) hospital community cloud and (v) Remote Base Station (RBS). The cloud-based framework worked on two modes: (i) Indoor-patient mode i.e. the patient is assumed to be inside the hospital, lies within the range of local servers which are linked to the hospital community cloud (ii) Outdoor-patient mode i.e. the patient is considered to be outside the hospital i.e. not within the range of local servers rather connected via RBS. Multi-biometric key generation approach is used to secure inter-sensor communication in WBANs for more secure and random key. Electronic Medical Records (EMRs) are used to store in the hospital community cloud for providing the security to data storage site and for preserving the privacy of the patient's data. The results revealed that this cloud-based framework is a practical and provably secure solution for mobile healthcare systems. This system is unique as it has offered a comprehensive cloud-based framework for WBANs.

4.3.4 Biometrics-based Cryptography Scheme for E-Health Systems

Chen et al. [104] proposed a biometrics-based cryptography scheme and has addressed the different security issues for E-Health system at various stages such as local communication, terminal processing, public communication and server processing. The authors addressed above issues by using Biometrics-based Fuzzy Authentication and Key Negotiation (BFAKN) and Fingerprint-based Authority Access Mechanism (FAAM). BFAKN is used for identity authentication, secure key negotiation and ensures authenticity of all the

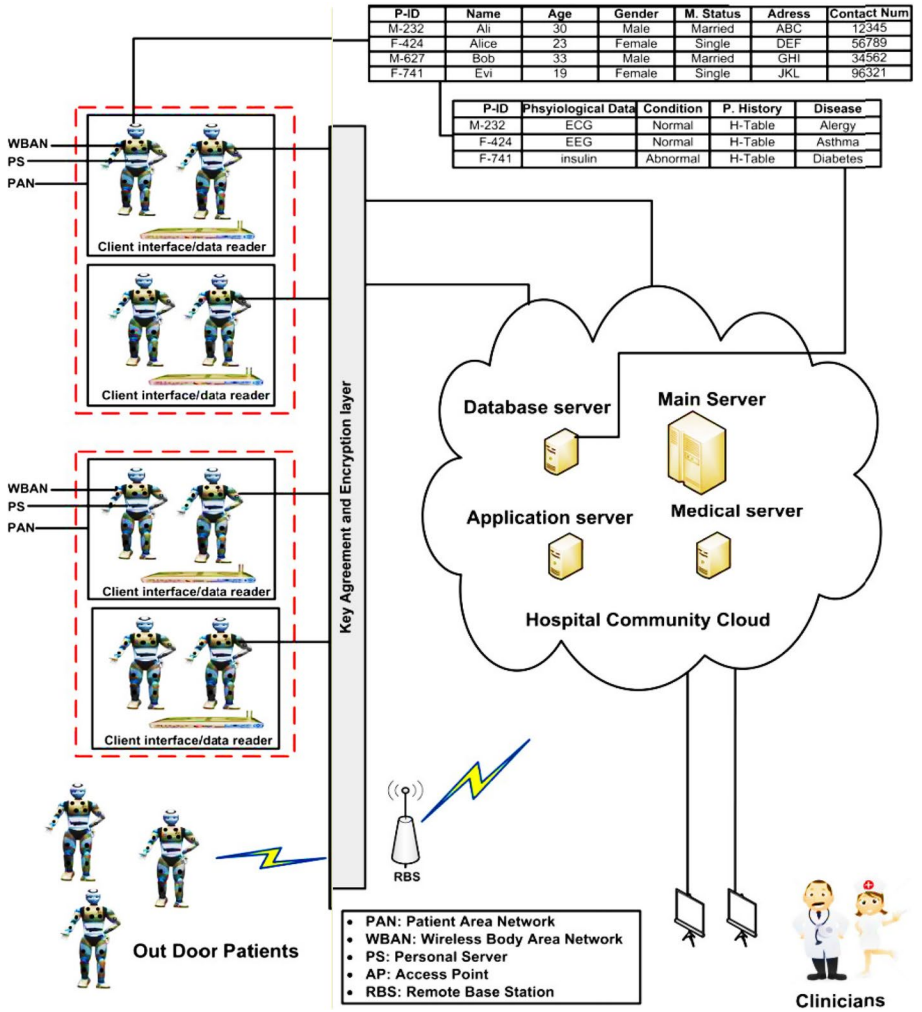

Fig. 13 Architecture of cloud based mobile healthcare system [103]

available components in the system. Juels and Sudan [105] presented a "fuzzy vault" algorithm for stable variability in biometrics.

The whole system consisted of three entities: (i) sensor nodes (ii) terminal (iii) monitoring centre i.e. medical staff with different authorities. Public communication links are established from terminal devices to the servers whereas local communication links are established from sensor nodes to the terminal devices. The fuzzy vault algorithm first received the biological signals, then extracted the various biometrics and generated a vault by using them. The vault is further transmitted to the receiver. The receiver can unlocked the vault by using its own biometric signals only if the signals are mutual with the sender. FAAM is used for providing the secure storage to data and for controlling the authorization access to patient data. The results have shown that this scheme has provided the high security and high performance.

4.3.5 Biometrics-based Key Establishment Protocol

Sammoud et al. [106] presented a biometric based key establishment protocol with minimal energy consumption for WBAN and optimized its performance. This protocol has created and shared a symmetric key by using ECG signal between two WBAN nodes. Bose-Chaudhuri-Hocquenghem (BCH) error correcting code is used for achieving identical sequences and for eliminating variation between two noted ECG signals. To ensure user confidentiality and privacy, morphing function is used for elimination of relation between the used symmetric keys and ECG signal. A third node is used for secure distribution of symmetric keys between two WBAN nodes. Selection of third node has a significant impact on the resource consumption and key establishment process. In this protocol, third node is chosen as the adjacent mutual ascendant of two nodes selected for key establishment. For optimisation of the consumed resources, time synchronisation is used. A temporary identifier (Idt) is assigned to each node for its use in key establishment process. This protocol consisted of two phases. In phase 1, each node shared a pre-fixed symmetric key with the sibling node in the mesh-tree topology except the root node. This phase is known as symmetric key establishment phase between parent and child. Phase 2 consisted of key generation between two children nodes having a common parent established a secure communication channel based on biometrics. The results indicated an optimal retrieval rate for this protocol. Through informal security analysis, the authors proved that this protocol is able to resist various security attacks viz. replay attack, key guessing attack, masquerade attack, eavesdropping, impersonation attack, MITM attack and forward/backward security. Formal security analysis of this protocol is carried out using ProVerif tool and Automated Validation of Internet Security Protocols and Applications (AVISPA). This protocol outperformed the SEKEBAN [99] and physiological feature based key agreement (PFKA) scheme [107] in terms of energy consumption but underperforms ECG linear prediction key agreement (ELPA) scheme [108]. In terms of key retrieval rate, this protocol and PFKA outperforms ELPA.

4.3.6 Comparison of Biometric Encryption Routing Protocols: Findings and Discussions

Randomness is the foremost requirement for good cryptographic keys and these are derived from random time varying signals such as biometrics. These signals contain high security so that any attacker could not guess the exact cryptographic key. A comparative analysis of different biometric encryption routing protocols in terms of goal, technique, pros, cons and other characteristics such as energy efficiency, computational overhead and security is given in Table 3.

The major challenge for SEKEBAN [99] is to implement conventional security infrastructures for WBAN. SEKEBAN is more energy efficient than SSL protocol [100] and Kerberos protocol [101]. Furthermore, it has shown 100% recoverability of key loss. The main disadvantage of [99] is security breach with device tampering. One of the main challenges for [102] is to present a low cost authentication scheme with no additional overhead. However, this framework is limited to tier-1(Intra WBAN) communication only. The key challenge for [103] is the need of highly secure framework for WBAN. This framework has shown high entropy than [59] but security breach can happen at tier-2 communication. For the authors of [104], the challenging part is to address and find solutions for different

Table 3 Biometric encryption routing protocols

Author	Mana et al. [99]	Wang et al. [102]	Khan et al. [103]	Chen et al. [104]	Sammoud et al. [106]
Name of protocol	SEKEBAN	Framework Using Wavelet-Domain HMM	Cloud-based framework	Cryptography Scheme for E-Health Systems	Biometrics-based key establishment protocol
Year	2009	2011	2014	2020	2020
Goal	To design secure and efficient key exchange method	To propose high performance authentication protocol	To evolve a secure, general and easily deployable mobile healthcare using cloud framework	To addresses different security issues for E-Health system at various stages	To design a reliable, secure and energy efficient protocol by using symmetric keys
Technique used	Morphing Block, Message Digest 5 (MD5), Handshake Protocol, MAC	Wavelet-Domain HMM, Hash, Selective Encryption approach	Cloud Framework, Discrete Wavelet Transform, MAC	BFAKN and FAAM	BCH, morphing function, Hashing function, Mac function
Security	Low	High	High	High	High
Results compared with other protocols	SSL protocol [100], Kerberos protocol [101], multipoint fuzzy key management [109, 110]	None	EKG-based key agreement [111]	None	SEKEBAN [99], PFKA scheme [107], ELPA scheme [108], multipoint fuzzy key management [109]
Biometric used in protocol	ECG	ECG	ECG, EEG (electroencephalogram)	Fingerprints, ECG, EEG	ECG
Key Update period	Fixed by the administrator	Short period of time as statistics of ECG remains same for short period	Short	Not Applicable	Short
Energy efficiency	Low	High	Not considered	Not considered	High
Key Recoverability	Yes	No	No	Yes	Yes
Ubiquitous access for patient data	No	No	Yes	Yes	Yes
Entropy of key	Low	Low	High	High	High
Computational overhead	Not considered	Low	Low	Low	Low

Table 3 (continued)

Author	Mana et al. [99]	Wang et al. [102]	Khan et al. [103]	Chen et al. [104]	Sammoud et al. [106]
Pros	Generates session key securely	Tolerate signal distortion	Provides privacy to patient data	False Acceptance Rate (FAR) is only 0.4% when error tolerance is 5	Low energy consumption than SEKEBAN [99] and PFKA scheme [107]
	Distributes session key securely	High authentication performance	Unique as cloud framework used for the first time	False Rejection Rate (FRR) can reach 6.5%	Highly Secure
	Secure end to end transmission	Time efficient model for data authentication	Highly secure	Highly secure	100% Key retrieval Rate
	Secure communication links between nodes	Elimination of initial key distribution phase	EMRs are securely stored	99.6% impersonation attack identification rate	FAR is 0.0%
	High recoverability of key loss	Low complexity	High entropy	Biometrics can hide a secret key with the help of fuzzy vault	FRR is 0.0%
	Energy efficient than [100] and [101]	Low cost encryption method		Unauthorized users cant access patient data	Optimal resource consumption
		Other biometric signal can be used		Reliable scheme for E-Health system	
Cons	Unique device Identifier (UId) acts as an initial shared secret key can be compromised	Limited to tier-1 communication only	Tier 2 communication can compromise the security	Energy efficiency parameter is not considered	High energy consumption than ELPA scheme [108]
	Device tampering compromised the security	Does not consider security of beyond WBAN communication			

security issues for E-Health system at various stages such as local communication, terminal processing, public communication and server processing. The key challenge for [106] is to design a secure biometrics-based routing protocol for the distribution of symmetric keys with optimal resource consumption.

On comparison of the biometric encryption protocols in terms of energy efficiency, security and overhead, the following conclusions are drawn. In terms of energy efficiency, [106] and [102] have shown high performance than [99] but [103] and [104] did not consider this important parameter. In terms of security for tier-1 (Intra WBAN) communication, [102–104] and [106] have performed better than [99]. As randomness is the primary requirement for good cryptographic keys, [103, 106] and [104] have performed better than [99] and [102]. All state-of-the-art approaches can withstand replay attack. However, for ubiquitous access of patient data, [103, 104] and [106] outperformed [99] and [102].

4.4 Hybrid Key Cryptographic Protocols

A hybrid security mechanism which combines both symmetric and asymmetric key cryptographic algorithms is a good choice for WBANs as symmetric key cryptographic algorithms need less computation resources and asymmetric key cryptographic algorithms are highly secure [112, 113]. In the following sections, various hybrid key cryptographic protocols presented during the last decade are discussed.

4.4.1 Hybrid Security Framework

Liu and Kwak [114] has introduced a hybrid security framework to fulfil the security needs of WBAN. Asymmetric key cryptography required a longer key size for same security strength and consumed more energy than symmetric key cryptography. Therefore, authors used asymmetric cryptographic methods only in the association process between sensor nodes and BC. The association protocols are of two types according to the various applications: (i) an association protocol using pre-shared master key and establishment of session key (ii) an association with ID-based Elliptic Curve Diffie-Hellman (ECDH) key exchange protocol and master key establishment. Symmetric key cryptographic algorithm, AES provided the link level security during data transmission after the reliable connection between sensor nodes and BC has been established. Three different modes of AES are used to provide security services in accordance with application requirements. This framework has shown a good trade-off between resource constraints and security of WBAN.

4.4.2 Secure and Quality of Service Assurance Scheduling Scheme

Medical data packets must have low waiting time during transmission as compared to other data packets. For this, Barua et al. [115] has studied various packet scheduling strategies that supported the real-time transmission and introduced an efficient secure data transmission mechanism with data integrity in WBAN. The data traffic has been classified into two categories (i) real-time traffic, (ii) non real-time traffic. It aided in lowering the average waiting time of the highly sensitive WBAN data traffic. This mechanism is user-centric. In this, symmetric key cryptography is used to share a secure key among all body sensors and for regular data encryption to cope up with energy and memory constraints of WBAN. Asymmetric key cryptography is used for session key management and digital signature based on bilinear pairing cryptography is preferred to ensure the data integrity. The

priority (or queue) of the WBAN traffic is based on its QoS requirements. Equations (5) and (6) represented the mathematical estimation of the average waiting time of the high priority queue (Q_h) and low-priority queue (Q_l) respectively. M/G/1 queuing system (where arrival of data packets are Markovian that uses Poisson distribution, service time uses General distribution and only single server present in system) is considered in this system. The numerical results revealed that this mechanism is secure, provided the data confidentiality and minimized the average waiting time of real-time data traffic.

$$E\left[W_h\right] = \frac{\rho_h \frac{L_h}{2R_h} + \rho_l \frac{L_h}{2R_h}}{1 - \rho_h} \tag{5}$$

$$E\left[W_l\right] = \frac{\rho_h \frac{L_h}{2R_h} + \rho_l \frac{L_h}{2R_h} + \rho_h E\left[W_h\right]}{1 - \rho_h - \rho_l} \tag{6}$$

where $E[W_h]$ and $E[W_l]$ is the expected waiting time of Q_h and Q_l respectively; R_h is the transmission rate and L_h is the packet length of the high priority queue (Q_h). The packets of Q_l and Q_h are called class-l (C_l) and class-h (C_h) packets are in service with probability ρ_l and ρ_h respectively.

4.4.3 Hybrid Authentication and Key Establishment Scheme

Drira et al. [116] has examined the heterogeneity between the architectural tiers of WBAN and presented a hybrid key agreement and authentication scheme. Symmetric key cryptography is utilized in nodes having limited resources such as actuator or sensor nodes. Identity-Based Cryptography (IBC) is an asymmetric key cryptography, used for communication between the Storage Site (SS) and the smart phone/Mobile Node (MN). The IBC has been preferred over traditional public key setup because it provided the simple private key generation and management system. IBC included the computation of public key, generation of private key to sign a message and verification of signature. The security of this scheme depended on the toughness of the Weak Diffie-Hellman (W-DH) problem. The security analysis illustrated that this scheme is robust against various attacks such as replay, DoS and MITM. Moreover, calculation load is reduced on sensor nodes as the authentication of mobile nodes is done by storage site. Thus, this scheme satisfied the resource constraints of WBAN.

4.4.4 Security Mechanism for Inter-WBAN and Intra-WBAN Communications

Key management is essential for enhancing the security of WBAN in its participating tiers. Irum et al. [117] has presented the hybrid key management scheme for both tier-1 and tier-2 WBAN communication that used both auto generation as well as the preloading of keys. When PS got compromised, there is preloading of only one key used in tier-1 communication and other keys are auto generated from electrocardiogram (ECG) signal due to its linear time complexity (O(n)) whereas tier-2 communication used the preloading-based technique that enhanced the security by removing the key exchange phase. Less number of keys is stored in the memory due to the memory constraints of sensor nodes. Thus, this method became competent in terms of both security and memory consumption of WBAN. The integrated approach of automatic key generation as well as preloading based technique

reinforced security. After analysis of storage requirements, security, energy and communication overhead, the results demonstrated major improvements over BARI + [118].

4.4.5 Secure Anonymous Authentication (AA) for WBAN

He et al. [119] reviewed the AA schemes for WBANs and concluded that these are not secure for e-healthcare applications. The authors have presented an impersonation attack and found that the AA scheme given by Liu et al. [89] is not secure against impersonation attack. Therefore, AA scheme has been introduced by taking consideration of various security requirements for WBANs. The network model consisted of three entities i.e. WBAN client (C), Network Manager (NM) and Application Provider (AP). The AA scheme comprised of three methods: initializing the system, registering the client to NM and authentication of client to AP. NM is a trusted third party that produced the system parameters and public/private keys of the AP's and store them at a secure and safe place. AP denoted a remote system and C got its secret key after registration with NM. Thus, AP and C could validate each other. In Liu et al.'s scheme [89] since AP is located in the hospital premises; it was easily prone to physical engineering attacks like tampering in memory data, firmware modification and many more. The impersonation attack can be ceased if data is stored in NM's database instead of AP's database for authentication purposes as suggested by AA scheme. The results demonstrated that the new AA scheme removed all security flaws in previous schemes with no extra computation cost. The computation cost of presented AA scheme at client side remained same as Liu et al.'s scheme [89].

4.4.6 Secure Health TeleMonitoring

National Institute for Science and Technology (NIST) [120] has suggested AES for low energy available networks due to its high data encryption rate and high speed. But the disadvantage of AES lies in its management of exchange of shared secret key. Hercigonja et al. [121] concluded that asymmetric cryptographic algorithms consume more memory and processing time but are highly secured than symmetric algorithms. Priya et al. [122] highlighted that the use of ECC algorithm alone consumed more processing time and computational power. Salim and Herba [123] has exploited the benefits of both symmetric and asymmetric encryption algorithms and presented a system consists of AES, RSA and Hash-based Message Authentication Code (HMAC). AES was used for encryption of patient data, RSA for protecting the shared secret key of AES and HMAC to protect data integrity of message. This system provided high level security but slower in processing because long bit keys are required in RSA which consumed more memory and energy. Basnet et al. [124] focused on minimizing the energy depletion in WBAN and provided high data encryption level using hybrid cryptography. They thoroughly studied the impact of hybrid AES and RSA algorithm on WBAN. For energy saving, the authors have chosen ECC algorithm over RSA and proposed the two energy modes. First, energy saving mode if residual energy of sensors is less than threshold energy and second energy rich mode if residual energy of sensors is greater than the threshold value. In energy rich mode, all three techniques AES, ECC and HMAC are followed but in energy saving mode, only AES and HMAC technique is used for encryption and integrity of patient data. Encryption time and energy consumption are two important parameters considered in the proposed

solution. Figure 14 illustrated the given hybrid encryption system for secure data transmission. Equations (7) and (8) presented the enhanced encryption system for the above given solutions.

$$Enhancedciphertext(EC) = ((((((P \oplus ky')Mr)Mc) \oplus ky') \tag{7}$$

$$Plaintext(P) = ((((((C \oplus ky')Mc)Mr) \oplus ky') \tag{8}$$

where $\oplus$ is XOR, ky' is secret key achieved from ECC, Plaintext (P), Mc is Mixed columns and Mr is Mixed rows. The secret key of AES algorithm has been created from ECC by using Eq. (9).

$$\mathrm{Ky}' = \mathrm{K} * \mathrm{P} \tag{9}$$

where K is a random number lies between 1 to (n–1), Ky′ is public key and P is point of elliptic curve.

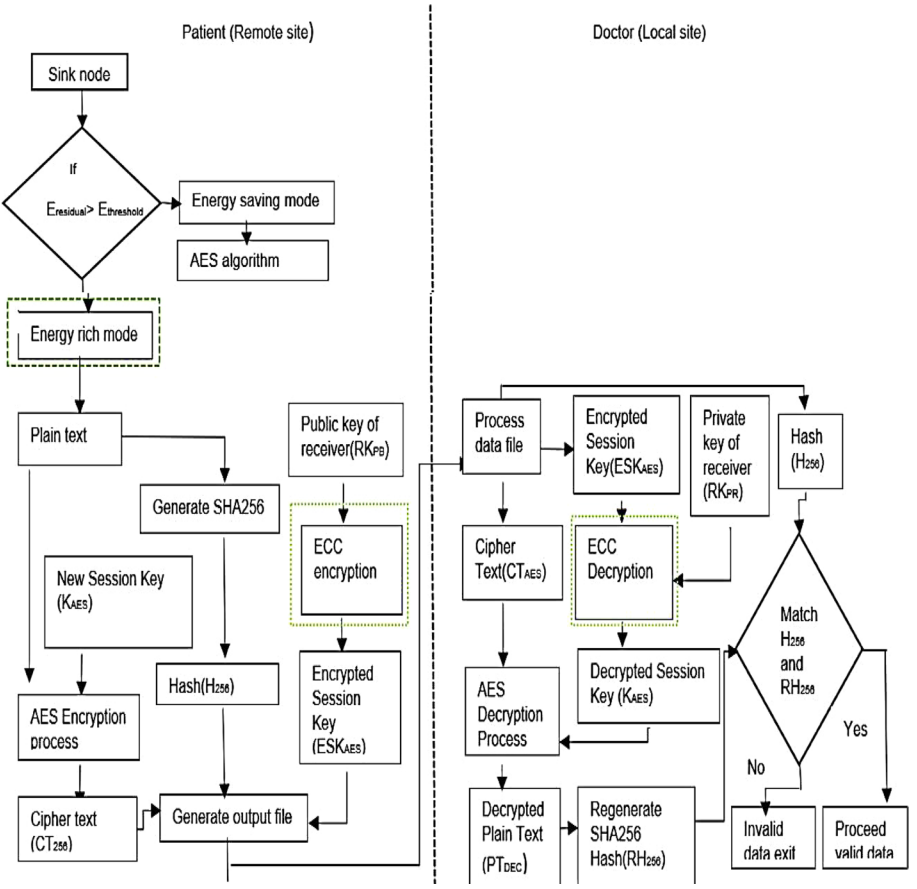

Fig. 14 Hybrid algorithm structure [124]

4.4.7 Comparative Study of Hybrid Key Cryptographic Protocols: Findings and Discussions

Security of patient data is the main challenge for WBAN for its worldwide acceptance. Various security approaches are reported in the literature for patient data protection. Nevertheless, WBAN face some difficulties because of resource constraints. Hybrid security mechanisms help to achieve high security in the wake of these constraints resulting in increased network lifetime. Comparative study of all hybrid key cryptographic protocols for WBANs in terms of their goal, pros, cons, techniques and other characteristics is summarized in Table 4.

The hybrid security framework [114] provided a feasible hybrid security structure satisfying various security requirements and resource constraints but did not consider the energy efficiency parameter. The major concern for [115] is to reduce the waiting time of real-time data traffic. Nevertheless, this scheme is user-centric and provided security to the patient data but it is prone to bilinear diffie -helman problem (BDHP). Moreover, throughput and energy consumption parameters are not considered. The challenge for [116] is to provide resilience against known security attacks and to reduce calculation load. In the process, the overall communication cost increased and security attributes got compromised at storage site. The major challenge faced by [117] is to achieve proficiency in terms of both memory utilization and security. This protocol outperformed in security, overall energy savings and communication overhead than BARI + [118] but at the expense of more energy consumption in the key refreshment phase. The authors of [119] achieved security in e-healthcare applications using AA scheme with no extra computation cost when compared to [89] and challenged the basic nature of AA schemes. Major challenges faced by [124] were minimization of energy consumption and encryption time. As compared to [123], this system is 11% faster in encryption process. Also, minimized the energy utilisation by 34%. The only disadvantage is increase in encrypted data file by more than 19% than original file.

By comparing the hybrid key cryptographic protocols in respect of data freshness, energy efficiency, security and computational overhead, the following conclusions are drawn. In terms of security of patient data, [116, 117, 119] and [124] have shown high performance than [114] and [115]. [124] has performed better than [117] in terms of energy efficiency. On the other hand, rest all state of art schemes [114–116] and [119] did not consider this important parameter. In terms of security [116, 117, 119] and [124] performed better than [114] and [115]. Prioritization of data traffic is considered only in [115]. Data freshness parameter is necessary for resilience against replay attack. It is considered in [114, 116, 117] and [119]. Size of encrypted data file remained same in all the mentioned schemes except [124]. [124] showed better results in lowering the encryption time than others. In terms of computational overhead, [117] outperformed all other schemes.

5 Conclusion and Future Scope

WBAN is a medical evolutionary technology for healthcare services. It provides continual monitoring, diagnosis and early prevention of various diseases. Furthermore, it helps to reduce healthcare costs. Nevertheless, the security and privacy issues hold it back for its successful implementation. Since, the physiological information of the patients is strictly

Table 4 Hybrid key cryptographic protocols

Author	Liu and Kwak [114]	Barua et al. [115]	Drira et al. [116]	Irum et al. [117]	He et al. [119]	Basnet et al. [124]
Name of protocol	Hybrid security framework	Secure and quality of service assurance scheduling scheme	Hybrid authentication and key establishment scheme	Security mechanism for intra-WBAN and inter-WBAN communications	Secure anonymous authentication (AA) for WBAN	Secure health telemonitoring
Year	2010	2011	2012	2013	2016	2019
Goal	To develop efficient and secure WBAN systems	To lower the waiting time of medical data packets	To propose a hybrid authentication and key establishment scheme	To strengthen security of tier-1 and tier-2 of WBAN	To propose a secure AA scheme having low cost	To improve security for real-time data communication in telemedicine
Technique used	AES, ID based ECC, and Diffie hellman	Bilinear pairing, Queue and digital signature	IBC, ECDH and Diffie–Hellman	Preloading of keys, biometric key generation, HMAC-MD5	ECC, Diffie Hellman, bilinear pairing	AES, ECC and HMAC
Security	Medium	Medium	High	High	High	High
Technique for initial key exchange phase	ID-based ECDH key exchange protocol	Bilinear Pairing	Identity-based signature	None	None	ECC
Energy efficiency	Not considered	Not considered	Not considered	Medium	Not considered	High
Data Freshness	Yes	Not considered	Yes	Yes	Yes	Not considered
Prioritization of data traffic	No	Yes	No	No	No	No
Computational overhead	Low	Low	Medium	Lowest	Low	Low

Table 4 (continued)

Author	Liu and Kwak [114]	Barua et al. [115]	Drira et al. [116]	Irum et al. [117]	He et al. [119]	Basnet et al. [124]
Pros	Usage of ECC rather than RSA	Minimize key storage space	Resilient to attacks such as DoS, replay and MITM	High entropy of EKG signal	Reduces computational cost at client side	Provides high data encryption level
	Fast cryptographic operation time	Need less computation	Efficient resource utilisation	Elimination of key exchange mechanism	Resilient to various attacks	Shorter encryption time
	Different modes of AES can be used for different security requirements	User centric scheme	Categorises nodes for trade-off between security and resource constraints	Easy Node Eviction	Stores patient's data in database of highly secure NM	More challenging to break down ECC than RSA
	Shows good trade-off between resource constraints and security	Consider priority based traffic	High authentication performance	Low Storage overhead than BARI+ [118]	Lower computational cost than Liu et al. [94] protocol	Increases network lifetime
	Fast computations	Ensures QoS for real time traffic	Low computational load on sensor nodes	Low communication overhead than [118]	Highly secure than previous AA schemes	Highly secure
Cons	Stringent Security requirements not met by AES	Bilinear Diffie-Hellman Problem (BDHP)	No security for data storage	Security of tier-3 not considered	Slightly higher communication cost than [94]	Size of encrypted file increases by 19%
	QoS parameters are not considered	QoS in group and peer to peer communication is not ensured	Usage of time consuming multiplication operation	More energy consumption in the key refreshment phase than [118]		No consideration of criticality of patient data and throughput

private and confidential, security mechanisms must be an integrated part of routing protocols of WBAN for its worldwide acceptance. However, designing of secure and energy efficient routing protocols is a challenging task due of its resource constrained nature. This paper has attempted to categorize the routing protocols of WBAN literature on the basis of different cryptosystems. After the analysis of each routing protocol, a comparative analysis is presented against other various schemes in terms of their goal, techniques, pros, cons and other characteristics. Various security and resource constrained challenges are taken into consideration in different classifications of protocols. It has been seen that symmetric key cryptographic routing protocols emphasise more on the resource constrained nature of WBAN than patient data security. On the other hand, asymmetric and biometric key cryptographic routing protocols emphasise more on security of patient data than resource constrained nature of WBAN. Hybrid key cryptographic routing protocols attempt to balance both the aspects.

The extensive literature survey suggests that future work should focus on network optimization to lower energy consumption, path loss and delay. Advanced and low overhead cryptographic techniques are recommended for meeting stringent security requirements in WBAN. Use of lossless compression techniques is suggested to reduce network traffic for achieving high throughput.

Authors' contributions NK–idea for the article, RS performed the literature search and drafted, RS and AB–performed data analysis, and DK & NK critically revised the work.

Funding None.

Availability of data and material Not applicable.

Code availability Not applicable.

Declarations

Conflict of interest The authors declared that they have no conflict of interest.

References

1. Suzman, R., & Beard, J. (2015). *Global health and aging: preface*. National Institute on Aging website.
2. American Hospital Association. (2007). *When I'm 64: How boomers will change health care* (pp. 00–10). Chicago: American Hospital Association.
3. Movassaghi, S., Abolhasan, M., Lipman, J., Smith, D., & Jamalipour, A. (2014). Wireless body area networks: A survey. *IEEE Communications Surveys & Tutorials, 16*(3), 1658–1686.
4. Fried, L. P., Ferrucci, L., Darer, J., Williamson, J. D., & Anderson, G. (2004). Untangling the concepts of disability, frailty, and comorbidity: Implications for improved targeting and care. *The Journals of Gerontology Series A: Biological Sciences and Medical Sciences, 59*(3), M255–M263.
5. Kulli, V. (2020). *The Management of the Development of a Geriatric-Friendly Practice Toolkit for Use in the Primary Care Setting: a Multi-Tiered Intervention to Improve the Health of Older Adults*. Doctoral dissertation, University of Pittsburgh.
6. Cypher, D., Chevrollier, N., Montavont, N., & Golmie, N. (2006). Prevailing over wires in healthcare environments: Benefits and challenges. *IEEE Communications Magazine, 44*(4), 56–63.
7. Honeine, P., Mourad, F., Kallas, M., Snoussi, H., Amoud, H., & Francis, C. (2011, May). Wireless sensor networks in biomedical: Body area networks. In *International Workshop on Systems, Signal Processing and their Applications, WOSSPA* (pp. 388–391). IEEE.

8. Van Dam, K., Pitchers, S., & Barnard, M. (2001). Body area networks: Towards a wearable future. In *Proceedings of WWRF kick off meeting, Munich, Germany, March 6–7, 2001*.
9. IEEE Standards Association. (2012). IEEE Standard for local and metropolitan area networks—Part 15.6: Wireless body area networks. *IEEE Standard for Information Technology, IEEE, 802*(6), 1–271.
10. Latré, B., Braem, B., Moerman, I., Blondia, C., & Demeester, P. (2011). A survey on wireless body area networks. *Wireless Networks, 17*(1), 1–18.
11. Bangash, J. I., Abdullah, A. H., Anisi, M. H., & Khan, A. W. (2014). A survey of routing protocols in wireless body sensor networks. *Sensors, 14*(1), 1322–1357.
12. Lohr, K. N., & Donaldson, M. S. (Eds.). (1994). *Health data in the information age: Use, disclosure, and privacy*. National Academies Press.
13. Pathania, S., & Bilandi, N. (2014). Security issues in wireless body area network. *Int J Comput Sci Mobile Comput, 3*(4), 1171–1178.
14. Raja, K. S., & Kiruthika, U. (2015). An energy efficient method for secure and reliable data transmission in wireless body area networks using RelAODV. *Wireless Personal Communications, 83*(4), 2975–2997.
15. Khan, Z. A., Sivakumar, S., Phillips, W., & Aslam, N. (2014). A new patient monitoring framework and energy-aware peering routing protocol (EPR) for body area network communication. *Journal of Ambient Intelligence and Humanized Computing, 5*(3), 409–423.
16. Lai, X., Liu, Q., Wei, X., Wang, W., Zhou, G., & Han, G. (2013). A survey of body sensor networks. *Sensors, 13*(5), 5406–5447.
17. Kaur, N., & Singh, S. (2017). Optimized cost effective and energy efficient routing protocol for wireless body area networks. *Ad Hoc Networks, 61*, 65–84.
18. Sangwan, A., & Bhattacharya, P. P. (2015). Wireless body sensor networks: A review. *International Journal of Hybrid Information Technology, 8*(9), 105–120.
19. Zriqat, I. A. A., & Altamimi, A. M. (2016). Security and privacy issues in eHealthcare systems: Towards trusted services. *International Journal of Advanced Computer Science and Applications, 7*(9), 229–236.
20. Javadi, S. S., & Razzaque, M. A. (2013). Security and privacy in wireless body area networks for health care applications. In S. Khan & A. S. K. Pathan (Eds.), *Wireless networks and security* (pp. 165–187). Springer.
21. Chunka, C., & Banerjee, S. (2021). An efficient mutual authentication and symmetric key agreement scheme for wireless body area network. *Arabian Journal for Science and Engineering*. https://doi.org/10.1007/s13369-021-05532-8
22. Devi, V. A., & Kalaivani, V. (2021). Enhanced BB84 quantum cryptography protocol for secure communication in wireless body sensor networks for medical applications. *Pers Ubiquit Comput*. https://doi.org/10.1007/s00779-021-01546-z
23. Azees, M., Vijayakumar, P., Karuppiah, M., et al. (2021). An efficient anonymous authentication and confidentiality preservation schemes for secure communications in wireless body area networks. *Wireless Networks*. https://doi.org/10.1007/s11276-021-02560-y
24. Alkhabet, M. M., & Ismail, M. (2021). Security algorithms for distributed storage system for E-health application over wireless body area network. *Journal of Ambient Intelligence and Humanized Computing*. https://doi.org/10.1007/s12652-020-02733-1
25. Ullah, I., Zeadally, S., Amin, N. U., Khan, M. A., & Khattak, H. (2021). Lightweight and provable secure cross-domain access control scheme for internet of things (IoT) based wireless body area networks (WBAN). *Microprocessors and Microsystems, 81*, 103477.
26. Nidhya, R., Shanthi, S., & Kumar, M. (2021). A novel encryption design for wireless body area network in remote healthcare system using enhanced RSA algorithm. In S. Satapathy, V. Bhateja, B. Janakiramaiah, & Y. W. Chen (Eds.), *Intelligent system design* (pp. 255–263). Springer.
27. Joshi, A., & Mohapatra, A. K. (2020). A novel lightweight authentication protocol for body area networks based on elliptic-curve cryptography. *Journal of Information and Optimization Sciences, 41*(7), 1645–1672.
28. Li, M., Lou, W., & Ren, K. (2010). Data security and privacy in wireless body area networks. *IEEE Wireless Communications, 17*(1), 51–58.
29. Liang, B., Liu, X., Zhou, H., Leung, V. C. M., Liu, A., & Chi, K. (2021). Channel resource scheduling for stringent demand of emergency data transmission in WBANs. *IEEE Transactions on Wireless Communications*. https://doi.org/10.1109/TWC.2020.3041471
30. Olatinwo, D. D., Abu-Mahfouz, A. M., & Hancke, G. P. (2021). Towards achieving efficient MAC protocols for WBAN-enabled IoT technology: A review. *Journal on Wireless Communications and Networking, 2021*, 60. https://doi.org/10.1186/s13638-021-01919-1

31. Liu, Q., Mkongwa, K. G., Zhang, C., et al. (2021). A simple cross-layer mechanism for congestion control and performance enhancement in a localized multiple wireless body area networks. *Journal of Ambient Intelligence and Humanized Computing*. https://doi.org/10.1007/s12652-020-02802-5
32. Touijer, B., Maissa, Y. B., & Mouline, S. (2021). IEEE 802.15. 6 CSMA/CA access method for WBANs: Performance evaluation and new backoff counter selection procedure. *Computer Networks, 188*, 107759.
33. Shen, G., Song, W., Gui, Y. and Gao, H., (2020) Access control for wireless body area networks. In: *International conference on security and privacy in new computing environments* (pp. 244–254). Springer, Cham.
34. Ibrahim, A.A. and Bayat, O., 2020, June. Medium Access Control Protocol-based Energy and Quality of Service routing scheme for WBAN. In *2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)* (pp. 1–6). IEEE.
35. La Manna, M., Perazzo, P., & Dini, G. (2021). SEA-BREW: A scalable attribute-based encryption revocable scheme for low-bitrate IoT wireless networks. *Journal of Information Security and Applications, 58*, 102692.
36. Al-Janabi, S., Al-Shourbaji, I., Shojafar, M., & Shamshirband, S. (2017). Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. *Egyptian Informatics Journal, 18*(2), 113–122.
37. Balasubramanyn, V.B., Thamilarasu, G. and Sridhar, R., (2007) Security solution for data integrity in wireless biosensor networks. In: *Distributed computing systems workshops, 2007. ICDCSW'07. 27th International Conference on* (pp. 79–79). IEEE.
38. Al Ameen, M., Liu, J., & Kwak, K. (2012). Security and privacy issues in wireless sensor networks for healthcare applications. *Journal of Medical Systems, 36*(1), 93–101.
39. Saba, T., Haseeb, K., Ahmed, I., & Rehman, A. (2020). Secure and energy-efficient framework using internet of medical things for e-healthcare. *Journal of Infection and Public Health, 13*(10), 1567–1575.
40. Alzubi, A., & Sari, A. (2016). Deployment of hash function to enhance message integrity in wireless body area network (WBAN). *International Journal of Communications, Network and System Sciences, 9*(12), 613.
41. Shanmugapriya, I., & Kumar, S. V. (2020). Pseudonym public key based sakai-kasahara certificateless signcryption for securing communication in WBAN. *Journal of Critical Reviews, 7*(6), 70–77.
42. Kumar, R., & Mukesh, R. (2013). State of the art: Security in wireless body area networks. *International Journal of Computer Science & Engineering Technology (IJCSET), 4*(05), 622–630.
43. Latif, R., Abbas, H., Latif, S., et al. (2016). Distributed denial of service attack source detection using efficient traceback technique (ETT) in cloud-assisted healthcare environment. *Journal of Medical Systems, 40*, 161. https://doi.org/10.1007/s10916-016-0515-4
44. Baskar, M., Ramkumar, J., Karthikeyan, C., et al. (2021). Low rate DDoS mitigation using real-time multi threshold traffic monitoring system. *Journal of Ambient Intelligence and Humanized Computing*. https://doi.org/10.1007/s12652-020-02744-y
45. Bengag, A., Bengag, A., & Moussaoui, O. (2020). Attacks classification and a novel IDS for detecting jamming attack in WBAN. *Advances in Science, Technology and Engineering Systems Journal, 5*(2), 80–86.
46. Arora K., Mahajan S. (2021) Detecting denial-of-service attack using dendritic cell approach. In D. Goyal, A.K. Gupta, V. Piuri, M. Ganzha, & M. Paprzycki (Eds.), *Proceedings of the second international conference on information management and machine intelligence. Lecture notes in networks and systems* (vol. 166). Singapore: Springer. https://doi.org/10.1007/978-981-15-9689-6_55.
47. Alsubaie, F, Al-Akhras, M and Alzahrani, H. A., (2020) Using machine learning for intrusion detection system in wireless body area network. In: *2020 First international conference of smart systems and emerging technologies (SMARTTECH), Riyadh, Saudi Arabia, 2020* (pp. 100–104). https://doi.org/10.1109/SMART-TECH49988.2020.00036.
48. Muhsin, Y. A., & Yassin, A. A. (2020). Design a lightweight authentication scheme for WBAN in healthcare systems. *Journal of Basrah Researches (Sciences), 46*(1), 160–170.
49. Corral-Plaza, D., Reich, O., Hübner, E., Wagner, M., & Medina-Bulo, I., (2019). A sensor fusion system identifying complex events for localisation estimation. In *Proceedings of the 16th international conference on applied computing*.
50. Sundar, S., Kumar, R., & Kittur, H. M. (2020). Improved indoor location tracking system for mobile nodes. *International Journal of Computer Aided Engineering and Technology, 12*(1), 1–16.
51. Healey, A. J., Fathi, P., & Karmakar, N. C. (2020). RFID Sensors in medical applications. *IEEE Journal of Radio Frequency Identification, 4*(3), 212–221. https://doi.org/10.1109/JRFID.2020.2997708

52. Poongodi, T., Rathee, A., Indrakumari, R., & Suresh, P. (2020). IoT sensing capabilities: Sensor deployment and node discovery, wearable sensors, wireless body area network (WBAN), data acquisition. In S. L. Peng, S. Pal, & L. Huang (Eds.), *Principles of internet of things (IoT) ecosystem: Insight paradigm* (pp. 127–151). Springer.
53. Cherukuri, S., Venkatasubramanian, K. K., & Gupta, S. K. (2003). BioSec: A biometric based approach for securing communication in wireless networks of biosensors implanted in the human body. In *Parallel processing workshops, 2003. Proceedings. 2003 International conference on* (pp. 432–439). IEEE.
54. Jegadeesan, S., Azees, M., Babu, N. R., Subramaniam, U., & Almakhles, J. D. (2020). EPAW: Efficient privacy preserving anonymous mutual authentication scheme for wireless body area networks (WBANs). *IEEE Access, 8*, 48576–48586. https://doi.org/10.1109/ACCESS.2020.2977968
55. Umar, M., Wu, Z., & Liao, X. (2021). Channel characteristics aware zero knowledge proof based authentication scheme in body area networks. *Ad Hoc Networks, 112*, 102374.
56. Tan, X., Zhang, J., Zhang, Y., Qin, Z., Ding, Y., & Wang, X. (2020). A PUF-based and cloud-assisted lightweight authentication for multi-hop body area network. *Tsinghua Science and Technology, 26*(1), 36–47.
57. Sowjanya, K., Dasgupta, M., & Ray, S. (2020). An elliptic curve cryptography based enhanced anonymous authentication protocol for wearable health monitoring systems. *International Journal of Information Security, 19*, 129–146. https://doi.org/10.1007/s10207-019-00464-9
58. Umar, M., Wu, Z., & Liao, X. (2020). Mutual authentication in body area networks using signal propagation characteristics. *IEEE Access, 8*, 66411–66422.
59. Rehman, Z. U., Altaf, S., & Iqbal, S. (2020). An efficient lightweight key agreement and authentication scheme for WBAN. *IEEE Access, 8*, 175385–175397.
60. Wang, C., Zheng, W., Ji, S., Liu, Q. and Wang, A., (2018). Identity-based fast authentication scheme for smart mobile devices in body area networks. Wireless Communications and Mobile Computing, 2018.
61. Chatterjee, K. (2019). An improved authentication protocol for wireless body sensor networks applied in healthcare applications. *Wireless Personal Communications, 111*, 1–19.
62. Kumar, P., & Lee, H. J. (2012). Security issues in healthcare applications using wireless medical sensor networks: A survey. *Sensors, 12*(1), 55–91.
63. Saleem, S., Ullah, S., & Kwak, K. S. (2011). A study of IEEE 802.15. 4 security framework for wireless body area networks. *Sensors, 11*(2), 1383–1395.
64. Roy, S., & Biswas, S. (2019). A novel trust evaluation model based on data freshness in WBAN. In *Proceedings of international ethical hacking conference 2018* (pp. 223–232). Singapore: Springer.
65. Saha, S., & Anvekar, D. K. (2017). A poly_hop message routing approach through node and data classification for optimizing energy consumption and enhanced reliability in WBAN. In: *2017 International conference on smart technologies for smart nation (SmartTechCon)* (pp. 788–792). IEEE.
66. Thomas, J. (2009). Medical records and issues in negligence. *Indian Journal of Urology: IJU: Journal of the Urological Society of India, 25*(3), 384.
67. Li, M., Lou, W., & Ren, K. (2010). Data security and privacy in wireless body area networks. *IEEE Wireless communications, 17*(1), 51–58.
68. Bruhadeshwar, B., Kothapalli, K., Poornima, M. and Divya, M., (2009). Routing protocol security using symmetric key based techniques. In: *2009 International conference on availability, reliability and security* (pp. 193–200). IEEE.
69. Saleem, S., Ullah, S., & Yoo, H. S. (2009). On the security issues in wireless body area networks. *JDCTA, 3*(3), 178–184.
70. Law, Y., Doumen, J., & Hartel, P. (2004). *Survey and benchmark of block ciphers for wireless sensor networks*. Technical Report TR-CTIT-04–07, Centre for Telematics and Information Technology. The Netherlands: University of Twente.
71. Sampangi, R.V., Dey, S., Urs, S.R. and Sampalli, S., (2012). A security suite for wireless body area networks. *arXiv preprint* arXiv:1202.2171
72. Baqai, A., Umrani, F. A., & Chowdhry, B. S. (2017). A novel protocol with patient and node identification for optical WBAN with inherent security and interference rejection. *Wireless Personal Communications, 95*(4), 4211–4224.
73. Baqai, A. (2014). Design, development and implementation of the IR signaling techniques for monitoring ambient and body temperature. *Mehran University Research Journal of Engineering and Technology, 33*(3), 365–366.
74. Kumar, P., & Sharma, A. (2018). Data security using genetic algorithm in wireless body area network. *International Journal of Advanced Studies of Scientific Research, 3*(9), 5.

75. Lin, C. H., Wu, J. X., Chen, P. Y., Li, C. M., Pai, N. S., & Kuo, C. L. (2021). Symmetric cryptography with a chaotic map and a multilayer machine learning network for physiological signal infosecurity: Case study in electrocardiogram. *IEEE Access, 9*, 26451–26467.
76. Pareek, N. K., Patidar, V., & Sud, K. K. (2013). Diffusion–substitution based gray image encryption scheme. *Digital Signal Processing, 23*(3), 894–901.
77. Norouzi, B., Seyedzadeh, S. M., Mirzakuchaki, S., & Mosavi, M. R. (2014). A novel image encryption based on hash function with only two-round diffusion process. *Multimedia Systems, 20*(1), 45–64.
78. Anwar, S., & Meghana, S. (2019). A pixel permutation based image encryption technique using chaotic map. *Multimedia Tools and Applications, 78*(19), 27569–27590.
79. San-Um, W., & Chuayphan, N. (2014). A lossless physical-layer encryption scheme in medical picture archiving and communication systems using highly-robust chaotic signals. In: *The 7th 2014 biomedical engineering international conference* (pp. 1–5). IEEE.
80. Telem, A. N. K., Segning, C. M., Kenne, G., & Fotsin, H. B. (2014). A simple and robust gray image encryption scheme using chaotic logistic map and artificial neural network. *Advances in Multimedia, 2014*, 19.
81. Yang, T.-L., Lin, C.-H., Chen, W.-L., Lin, H.-Y., Chen-San, Su., & Liang, C.-K. (2019). Hash transformation and machine learning-based decision-making classifier improved the accuracy rate of automated Parkinson's disease screening. *IEEE Transactions on Neural Systems and Rehabilitation Engineering, 28*(1), 72–82.
82. Yang, T. L., Kan, P. J., Lin, C. H., Lin, H. Y., Chen, W. L., & Yau, H. T. (2019). Using polar expression features and nonlinear machine learning classifier for automated Parkinson's disease screening. *IEEE Sensors Journal, 20*(1), 501–514.
83. Wu, J. X., Chen, P. Y., Li, C. M., Kuo, Y. C., Pai, N. S., & Lin, C. H. (2020). Multilayer fractional-order machine vision classifier for rapid typical lung diseases screening on digital chest X-Ray images. *IEEE Access, 8*, 105886–105902.
84. Chougrad, H., Zouaki, H., & Alheyane, O. (2018). Deep convolutional neural networks for breast cancer screening. *Computer Methods and Programs in Biomedicine, 157*, 19–30.
85. Li, T. H. S., Liu, C. Y., Kuo, P. H., Fang, N. C., Li, C. H., Cheng, C. W., Hsieh, C. Y., Wu, L. F., Liang, J. J., & Chen, C. Y. (2017). A three-dimensional adaptive PSO-based packing algorithm for an IoT-based automated e-fulfillment packaging system. *IEEE Access, 5*, 9188–9205.
86. SB-Projects: IR remote control, Sony SIRC Protocol, http://www.sbprojects.com/knowledge/ir/sirc.php. Accessed 22 December 2014.
87. Darwish, A., & Hassanien, A. E. (2011). Wearable and implantable wireless sensor network solutions for healthcare monitoring. *Sensors, 11*(6), 5561–5595.
88. He, D., & Zeadally, S. (2015). Authentication protocol for an ambient assisted living system. *IEEE Communications Magazine, 53*(1), 71–77.
89. Liu, J., Zhang, Z., Chen, X., & Kwak, K. S. (2013). Certificate less remote anonymous authentication schemes for wireless body area networks. *IEEE Transactions on Parallel and Distributed Systems, 25*(2), 332–342.
90. Zhao, Z. (2014). An efficient anonymous authentication scheme for wireless body area networks using elliptic curve cryptosystem. *Journal of Medical Systems, 38*(2), 13.
91. Perkins, C., Belding-Royer, E., & Das, S. (2003). Ad hoc on-demand distance vector (AODV) routing (No. RFC 3561) Google Scholar.
92. Manfredi, S. (2012). Reliable and energy-efficient cooperative routing algorithm for wireless monitoring systems. *IET Wireless Sensor Systems, 2*(2), 128–135.
93. Li, X., Peng, J., Kumari, S., Wu, F., Karuppiah, M., & Choo, K. K. R. (2017). An enhanced 1-round authentication protocol for wireless body area networks with user anonymity. *Computers & Electrical Engineering, 61*, 238–249.
94. Liu, J., Zhang, L., & Sun, R. (2016). 1-Raap: An efficient 1-round anonymous authentication protocol for wireless body area networks. *Sensors, 16*, 728.
95. Xiong, H., & Qin, Z. (2015). Revocable and scalable certificateless remote authentication protocol with anonymity for wireless body area networks. *IEEE Transactions on Information Forensics and Security, 10*(7), 1442–1455.
96. Singla, R., & Kaur, N. (2018). Compressed and secure energy efficient routing protocol for WBAN. *International Journal of Computer Sciences and Engineering, 6*(7), 254–260.
97. Malmivuo, J., & Plonsey, R. (1995). *Bioelectromagnetism: Principles and applications of bioelectric and biomagnetic fields*. Oxford University Press.

98. Guennoun, M., Zandi, M., & El-Khatib, K. (2008). On the use of biometrics to secure wireless biosensor networks. In: *2008 3rd International conference on information and communication technologies: From theory to applications* (pp. 1–5). IEEE.
99. Mana, M., Feham, M., & Bensaber, B. A. (2009). SEKEBAN (Secure and Efficient Key Exchange for wireless Body Area Network). *International Journal of Advanced Science and Technology*.
100. Haque, M. M., Pathan, A. S. K., & Hong, C.S. (2008). Securing U-healthcare sensor networks using public key based scheme. In: *2008 10th International conference on advanced communication technology* (Vol. 2, pp. 1108–1111). IEEE.
101. Großschädl, J., Szekely, A., & Tillich, S. (2007). The energy cost of cryptographic key establishment in wireless sensor networks. In: *Proceedings of the 2nd ACM symposium on information, computer and communications security* (pp. 380–382).
102. Wang, H., Fang, H., Xing, L., & Chen, M. (2011). An integrated biometric-based security framework using wavelet-domain HMM in wireless body area networks (WBAN). In: *2011 IEEE international conference on communications (ICC)* (pp. 1–5). IEEE.
103. Khan, F. A., Ali, A., Abbas, H., & Haldar, N. A. H. (2014). A cloud-based healthcare framework for security and patients' data privacy using wireless body area networks. *Procedia Computer Science, 34*, 511–517.
104. Chen, H., Ding, D., Su, S. and Yin, J., (2020). Biometrics-based cryptography scheme for E-Health systems. In: *Journal of Physics: Conference Series* (Vol. 1550, p. 022039). IOP Publishing.
105. Juels, A., & Sudan, M. (2002) A fuzzy vault scheme. In: *IEEE International symposium on information theory* (pp. 408–415). Lausanne.
106. Sammoud, A., Chalouf, M. A., Hamdi, O., Montavont, N., & Bouallegue, A. (2020). A new biometrics-based key establishment protocol in WBAN: Energy efficiency and security robustness analysis. *Computers & Security, 96*, 101838.
107. Jammali, N., & Fourati, L.C. (2015). PFKA: A physiological feature based key agreement for wireless body area network. In *2015 International conference on wireless networks and mobile communications (WINCOM)* (pp. 1–8). IEEE.
108. Zaghouani, E. K., Jemai, A., Benzina, A. and Attia, R., (2015). ELPA: A new key agreement scheme based on linear prediction of ECG features for WBAN. In: *2015 23rd European signal processing conference (EUSIPCO)* (pp. 81–85). IEEE.
109. Bui, F. M., & Hatzinakos, D. (2007). Biometric methods for secure communications in body sensor networks: Resource-efficient key management and signal-level data scrambling. *EURASIP Journal on Advances in Signal Processing, 2008*, 1–16.
110. Poon, C. C., Zhang, Y. T., & Bao, S. D. (2006). A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. *IEEE Communications Magazine, 44*(4), 73–81.
111. Venkatasubramanian, K.K., Banerjee, A. and Gupta, S.K., (2008). EKG-based key agreement in body sensor networks. In: *IEEE Infocom Workshops 2008* (pp. 1–6). IEEE.
112. Farooq, S., Prashar, D., & Jyoti, K. (2018). Hybrid encryption algorithm in wireless body area networks (WBAN). In R. Singh, S. Choudhury, & A. Gehlot (Eds.), *Intelligent communication, control and devices* (pp. 401–410). Springer.
113. Pan, J., Li, S., & Xu, Z. (2012). Security mechanism for a wireless-sensor-network-based healthcare monitoring system. *IET Communications, 6*(18), 3274–3280.
114. Liu, J., & Kwak, K. S. (2010). Hybrid security mechanisms for wireless body area networks. In: *Ubiquitous and future networks (ICUFN), 2010 Second international conference on* (pp. 98–103). IEEE.
115. Barua, M., Alam, M. S., Liang, X., & Shen, X. (2011, March). Secure and quality of service assurance scheduling scheme for wban with application to ehealth. In *2011 IEEE Wireless Communications and Networking Conference* (pp. 1102–1106). IEEE.
116. Drira, W., Renault, E. and Zeghlache, D., (2012). A hybrid authentication and key establishment scheme for wban. In: *Trust, security and privacy in computing and communications (TrustCom), 2012 IEEE 11th international conference on* (pp. 78–83). IEEE.
117. Irum, S., Ali, A., Khan, F. A., & Abbas, H. (2013). A hybrid security mechanism for intra-WBAN and inter-WBAN communications. *International Journal of Distributed Sensor Networks, 9*(8), 842608.
118. Muhammad, K.-U.R.S., Lee, H., Lee, S., & Lee, Y.-K. (2010). BARI+: A biometric based distributed key management approach for wireless body area networks. *Sensors, 10*(4), 3911–3933.
119. He, D., Zeadally, S., Kumar, N., & Lee, J. H. (2016). Anonymous authentication for wireless body area networks with provable security. *IEEE Systems Journal, 11*(4), 2590–2601.
120. Amin, R., Islam, S. H., Biswas, G. P., Khan, M. K., & Li, X. (2015). Cryptanalysis and enhancement of anonymity preserving remote user mutual authentication and session key agreement scheme for e-health care systems. *Journal of Medical Systems, 39*(11), 140.

121. Hercigonja, Z. (2016). Comparative analysis of cryptographic algorithms. *International Journal of Digital Technology & Economy, 1*(2), 127–134.
122. Priya, C. L., & Visalakshi, U. S. (2017). Secure and efficient communication using ECC algorithm in wireless body area network. *International Journal of Engineering Science, 7*, 10073.
123. Harba, E. S. I. (2017). Secure data encryption through a combination of AES, RSA and HMAC. *Engineering, Technology & Applied Science Research, 7*(4), 1781–1785.
124. Basnet, A., Alsadoon, A., Prasad, P. W. C., Alsadoon, O. H., Pham, L., & Elchouemi, A. (2019). A novel secure patient data transmission through wireless body area network: Health tele-monitoring. *International Journal of Communication Networks and Information Security, 11*(1), 93–104.

Ripty Singla obtained her B.Tech. and M.Tech (Computer Engg.) degree from Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib, Punjab in 2016 and 2018 respectively. She is working as Assistant Professor, Department of Computer Science & Engineering in Chandigarh University, Mohali, Punjab, India. Her current research interests include Wireless Sensor Networks, Soft Computing, Deep Learning and Wireless Body Area Networks.

Navneet Kaur obtained her B.Tech. (Computer Engg.) degree from Panjab Technical University, Jalandhar in 2000,M.E. (Computer Sc. &Engg.) Hons. and Ph.D Degree from Panjab University, Chandigarh in 2007 and 2018 respectively. She is working as Professor in the Department of Computer Science and Engineering in Chandigarh University, Mohali, Punjab, India. She is the Life Member of CSI and Member of ACM and IEEE. Her research interests include Wireless Sensor Networks, Wireless Body Area Networks and Wireless Adhoc Networks.

Deepika Koundal is currently associated with University of Petroleum and Energy Studies, Dehradun. She is having 12 years of teaching and research experience at various reputed Universities of India. She was previously associated with NIT Hamirpur as an Assistant Professor. Prior to that she worked at UIET, Panjab University, Chandigarh. She received her B.Tech. Degree in Computer Science and Engineering from Kurukshetra University, Kurukshetra, Haryana, India and subsequently her M.E. and Ph.D. Degrees in Computer Science & Engineering from UIET, Panjab University, Chandigarh, India. Her Ph.D. thesis is focused on Healthcare domain. She is the awardee of Research excellence award given by Chitkara University in 2019. She also received the recognition and honorary membership from Neutrosophic Science Association from University of Mexico. She has published more than 30 research articles in reputed SCI and scopus indexed journals, conferences and two books. She is a guest editor in Journal titled Computer & Electrical Engineering. Her research interests include Wireless Sensor Networks, Wireless Body Area Networks, Image processing in healthcare and agriculture domain.

Anuj Bhardwaj M. Tech. & Ph. D degree in Computer Science & Engineering. He is currently a Professor of Computer Science & Engineering with Chandigarh University, Mohali, Punjab. He is having a long experience of 15+ years in the field of industry and academics. He is having 36+ international papers in reputed conferences and journals. He has contributed 4 books with publishers like Nerosa and Alpha, Taylor & Francis Group and currently working on 3more accepted books. He had also contributed 6 chapters for reputed publishers. His current research interests include pattern & character recognition, graphics & vision, artificial intelligence & neural networks and machine learning.