INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

REVIEW ARTICLE

Secured Key Agreement Schemes in Wireless Body Area Network — A Review

S Z Hussain[1], **Manoj Kumar**[1]*

1 Department of Computer Science, Jamia Millia Islamia, New Delhi, India

OPEN ACCESS

Received: 03.01.2021

Accepted: 02.06.2021

Published: 13.07.2021

Citation: Hussain SZ, Kumar M (2021) Secured Key Agreement Schemes in Wireless Body Area Network — A Review. Indian Journal of Science and Technology 14(24): 2005-2033. https://doi.org/10.17485/IJST/v14i24.1708

* **Corresponding author**.

manoj.rke77@gmail.com

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Objective: To review different key agreement schemes which are used to establish Wireless body area network (WBAN) on the basis of identified attacks and also evaluate the schemes on performance parameters. **Method**: In this paper, an overview of WBAN, its architecture, difference between WSN and WBAN, IEEE 802.15.6 specifications of WBAN, attacks in the environment and security essentials are discussed at first. It further divides the key agreement schemes into four classes and provides an extensive review of the schemes on the basis of distinct parameters viz. data confidentiality, node authentication, data integrity, mutual authentication, unforgeability, unlinkability, forward/backward secrecy, scalability, freshness, dos attack and node capture attack. Schemes are searched using the keywords- ("Traditional Key Agreement Scheme" OR "Physiological Key Agreement Scheme" OR "Signal Based Key Agreement Scheme" OR "Hybrid Key Agreement Scheme" OR "Security in Key Agreement Scheme") AND ("Wireless Body Area Network" OR "WBAN" OR "Body Area Network" OR "BAN" OR "Body Sensor Network" OR "BSN" OR "Medical Body Area Network" OR "MBAN"). The papers are shortlisted around long stretches of 2003-2021 with a focus on recent work from IEEE Xplore, Springer, Science Direct, ACM, MDPI and Google Scholar databases. Schemes are analyzed against the mentioned attacks and the result of the comparative analysis is shown using tables and chart tools graphically. **Findings**: The wide coverage of the schemes in this review provides in-depth exposure to the shortcomings of the different schemes against the listed attacks which will provide a road map to the researchers to develop secure schemes in the future. Moreover, maximum schemes do not consider all the three aspects of performance viz. memory efficiency, computational efficiency and energy efficiency which are the foremost parameters in resource scarce environment of WBAN. **Novelty**: This review is unique as it analyzes the distinct key agreement schemes under specific attacks found in the literature while other review papers discuss the general aspects of the security threats and corresponding counter measures in WBAN environment. It also provides the performance analysis of the key management schemes which are missing from other review works.

Keywords: WBAN; IOT; Bio sensors; Security; Privacy; Attacks; Encryption; Key agreement schemes; IEEE 802.15.6

1 Introduction

With the advancement in electronics and embedded systems, the size of the bio-sensors has been reduced to a level that now it is possible to wear these sensors either on the clothing or body or even implanted inside the body[1]. Considering the continuous growth in world population, improving life expectancy, growing chronic diseases, increasing use of bio-sensors in sports and rising popularity of medical device in personal fitness; wearable medical devices will see a sharp increase in its usage globally[2]. IOT is creating wave in personal fitness and it is going to be one of the strongest market as per different surveys. According to a market research company named IOT ANALYTICS; the number of IOT devices are expected to be 10 billion by 2020 and 22 billion by 2025[3]. The global market of wearable medical devices was evaluated worth USD 445.6 million in 2017. The overall market is predicted to observe a CAGR of about 17% for the duration of the forecast period 2018-23[4,5]. Wearable sensors are larger in size consequently having a bigger battery, more computational resources and larger storage in comparison to implantable sensors. Wearable sensors are generally used to measure blood pressure, heart rate, glucose level, respiration, pulse oximeter SpO_2, temperature and pH level whereas implantable devices are used to measure brain liquid pressure, cardiac arrhythmia and endoscopy[6]. The invasive body sensors are small, thin, wireless enabled and operate at low power.

A basic architecture of WBAN based on IOT is shown in Figure 1[7]. The entire architecture is divided in three tiers. Tier 1 is responsible for intra-BAN communication whereas Tier 2 is responsible for inter-BAN communication. Tier 3 represents the already established network and responsible for beyond BAN communication. The wearable or implanted bio-sensors are called nodes and create an intra-BAN network with one node acting as a personal server.

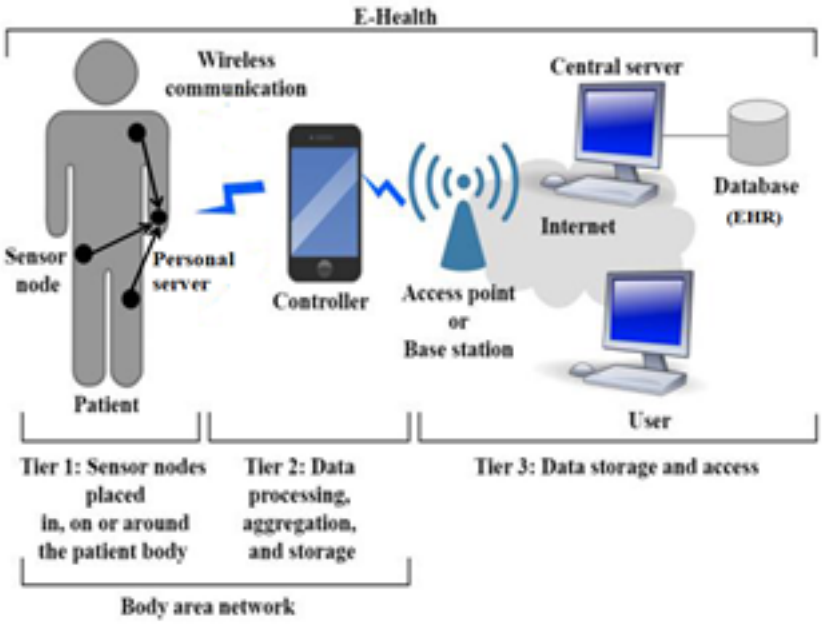

Fig 1. IOT based Healthcare Architecture

Literature on WBANs describes either a star topology or a multi-hop topology for communicating the nodes to personal server as shown in Figure 2 [8]. Considering the small size of WBAN, a star topology may be a reasonable option in which all the nodes are directly connected to the personal server without any intermediate nodes in between. Alternative approach in WBAN is multi-hop communication. Nodes need not connect directly with personal server but connect using one or two hops. Muti-hop communication is a better approach in case the nodes are using very low power radios producing low transmission range and low wireless channel quality. The con of multi-hop communication is that it requires routing and may suffer from longer latencies.

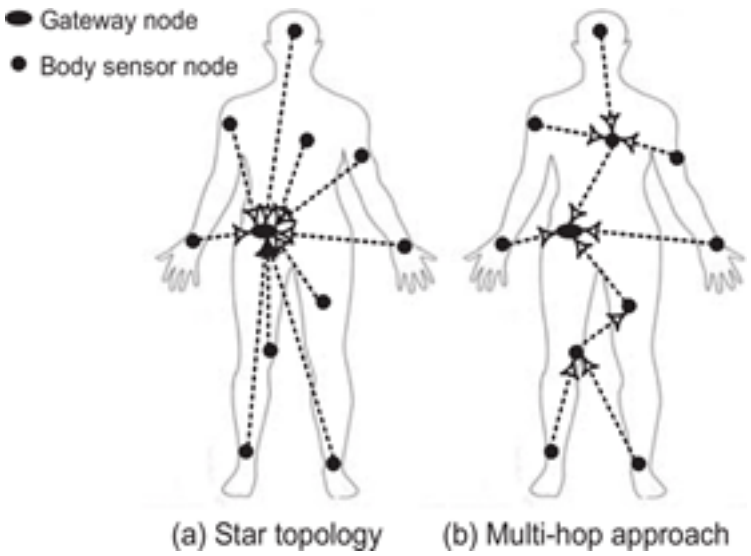

Fig 2. Star topology and Multi-hop Topology

Personal server collects the data from different nodes and pass on to the mobile device or PDA [9]. There could be related healthcare application developed and installed on mobile device. The rapid growth of Smartphone plays a crucial role in the implementation of WBAN. These collected values may be compared in real time with the threshold values already stored in healthcare app in mobile. When the values cross the threshold limit with a significant margin, the case must be reported immediately to the caregivers or a medical response team to handle the paroxysmal sickness thus arises in life critical situations. In common situation, the mobile app transmits the collected data to a centralized server periodically for permanently storage in electronic healthcare repository (EHR). The recorded medical information is used for long term storage in EHR which acts as an online database for clinical diagnosis, experts' advice and for future references [10].

The field aims to connect millions of healthcare IOT devices for remote monitoring in near future which shows that massive amount of data would be generated. This explosion of data would cause several challenges in IOT implementation. Security would pose the biggest threat among others. 70% of IOT devices contain insufficient authorization and severe vulnerabilities [11]. Identity preservation, secured data transportation, insecure web interfaces and database repository, inadequate software application protection and insufficient authorization are the major threats in the implementation of WBAN which can put the life of an individual in danger. An attack on WBAN can suppress the legitimate data leading to unwanted action in terms of wrong drug delivery by actuator or not informing the doctor in case of life critical situation. Also, personal health related information must not be accessible to an unauthorized one. Traditional cryptographic methods cannot be applicable in IOT based WBAN as the environment is extremely resource constrained in terms of computation capacity, storage and battery power. Adequate authentication methods, compatible firewalls, strong encryption techniques and other safeguards are required to be evolved to strengthen the system. In case of invasive bio-sensors, entire system is expected to exchange minimum messages transmission which would keep the temperature of the body in control otherwise it can damage the tissues [12,13]. Security issues and privacy concerns must be taken care on priority before making any disaster to happen in the society [14].

Considering the security viewpoint of WBAN in focus, research can be divided as into three different tiers as follows

1. Security aspects in intra-WBAN transmission (Tier 1 of WBAN architecture)
2. Security aspects in Inter-WBAN transmission (Tier 2 of WBAN architecture)
3. Security aspects in Beyond-WBAN transmission (Tier 3 of WBAN architecture)

Intra-BAN communication (Tier 1) confers the communication with the body sensors and personal server (Figure 1). The data gathered on personal server is communicated to nearby linked device or PDA in tier 2. This communication is found to be heterogeneous and required to be protected. The collected medical data is sent to store in Electronic Health Repository (EHR) at web server in tier 3. The data in exchange and storage in EHR at web server is also required to be protected. This paper covers the security key agreement schemes required in intra-WBAN architecture which is the primary aspect of security in tier 1.

Several review papers on security of Wireless Body Area Network (WBAN) are available in the literature. The common aspect in many of the papers is discussing the security threats and the corresponding countermeasures. The three basic security principles Confidentiality, Integrity and Availability (CIA) are discussed in Mainanwal et al.[15], Al-Janabi et al.[16], Usman et al.[17]. General security requirements such as data freshness and secure management are discussed in Al-Janabi et al.[16]. Different types of attacks on WBAN are also discussed in the literature. A set of protocol stack layer attacks are discussed in Bharathi and Venkateswari[18] while Kompara and Hölbl[19] discuss a set of eighteen different types of active and passive attacks. Authentication is briefly reviewed in Mainanwal et al.[15], Al- Janabi et al.[16] and Usman et al.[17] while different authentication schemes are discussed in Chaudhary et al.[20]. A detailed survey on key agreement schemes in WBAN along with security evaluation methods is provided in Kompara and Hölbl[19]. Security challenges on different tiers of WBAN are provided in Usman et al.[17]. Hasan et. al.[21] focuses the pitfall of WBAN architecture, security, reliability, classification & applications of WBAN including medical & non-medical applications. Jabeen, T. et al.[22] provides a comparison of multiple data security schemes for WBAN considering different attack scenarios. Their work is restricted only on performance analysis of different schemes in terms of time, cost and memory range. Liu et. al[23] discuss that the attacks on BAN may degrade the performance of WBAN in terms of increased network congestion, higher energy consumption and higher delays besides inaccurate data communication which leads to erroneous healthcare decisions.

It is found that very less focus is stressed on the key agreement schemes in WBAN in the literature and the available reviews are either old or limit themselves to portray a complete analysis of the schemes under the specific security parameters identified in the literature and their corresponding performance analysis. There is a great need to take stock of the accumulation of recent developments in this area. This review work fills the research gap found in the available literature. It is an improvement over the past reviews on key agreement schemes in WBAN which are first and foremost agenda in securing WBAN.

This work first categorizes the key agreement schemes into different groups depending upon their nature. Schemes are analyzed based upon identified parameters related to security countermeasures viz. data confidentiality, node authentication, data integrity, mutual authentication, unforgeability, unlinkability, forward/backward secrecy, scalability, freshness, dos attack and node capture attack. It further investigate the schemes on performance related parameters viz. usage of hash technique, usage of symmetric/ asymmetric key, memory efficiency, computational efficiency and energy efficiency. Unlike other review papers which cover the general aspects of the security requirements in WBAN, this work provides a detailed review which covers a range of key agreement schemes since almost the inception of WBAN up to the latest. This work is unique as the authors of this paper could not come across any other systematic literature reviews on key agreement schemes which are so extensive in nature.

The main contribution of this work is as follows-

1. A concise introduction of WBAN architecture in compliance with IEEE 802.15.6 standard which offers an entry level to the research area.
2. Discuss the attacks and security requirements of WBAN especially at tier-1 and tier-2.
3. To develop the taxonomy covering key agreement schemes in WBAN environment. The surveyed schemes are discussed against the different attacks in each part of taxonomy.
4. All the schemes are analyzed critically in the purview of eleven attacks which are identified on the basis of literature review. It will motivate the researchers for providing efficient solutions to the indicated problems.
5. Performance analysis of all the schemes is also conducted.
6. In each taxonomy, tables are used to show the comparative analysis and chart tools to depict the result graphically.
7. Research opportunities, directions and open issues in WBAN are also discussed.

In this paper, the architecture of the WBAN is discussed first. The rest of the paper is organized as follows. The methodology of the review is discussed in section 2. The differences between WSN and WBAN are discussed in section 3. Section 4 elaborates the IEEE standard for WBAN i.e. IEEE 802.15.6. Different types of possible Attacks on BAN are discussed in Section 5. Security requirements are identified and discussed in Section 6. Different key agreement schemes are elaborated in Section 7. Section 8 provides an analysis of key agreement schemes on the basis of different parameters and Section 9 provides the conclusion.

2 Methodology

This section provides a systematic review methodology of the literature relevant to key agreement schemes in WBAN environment. In this article, systematic review is performed to collect subsidiary information by dividing the entire process in two levels.

2.1 Inceptive Level

It is an initial phase for the appraisal of the research which includes the identification of the research question, suitable keywords to search reference papers from database libraries, period of coverage, inclusion and forbidden criteria.

Research Question

Research question contains the core requirement. This manuscript is aimed to contribute the answer to the following question. Question: What are the security essentials in the development of key agreement schemes in intra-BAN communication of WBAN architecture, their limitations, challenges and performance evaluation in the purview of different possible attacks?

Search Keywords

An important task is to generate the multiple strings for searching which do not leave anything from the research question. Important expressions are produced by joining diverse words. Words are also substituted without diluting their meaning. To find the articles related to our research domain, the following search strings are employed-
("Traditional Key Agreement Scheme" OR "Physiological Key Agreement Scheme" OR "Signal Based Key Agreement Scheme" OR "Hybrid Key Agreement Scheme" OR "Security in Key Agreement Scheme") AND ("Wireless Body Area Network" OR "WBAN" OR "Body Area Network" OR "BAN" OR "Body Sensor Network" OR "BSN" OR "Medical Body Area Network" OR "MBAN").

Research paper selection from database libraries

Digital libraries are searched using the mentioned search keywords precisely to identify the most relevant research articles. The research papers are selected from the databases enlisted in Table 1.

Table 1. Database Libraries

Publisher	URL	No. of Papers
IEEE Xplore	http://ieeexplore.ieee.org/	52
Springer	https://www.springer.com/gp	25
Science Direct-Elsevier	https://www.elsevier.com/en-in	15
ACM	https://www.acm.org/	11
MDPI	https://www.mdpi.com/	5
Google Scholar	https://scholar.google.com/	23

Period of Coverage

The exploration of WBAN key agreement schemes around long stretches of 2003-2021. The quantity of papers is specified in Table 1 and their detailed discussion is included in the following sections.

Inclusion and forbidden criteria

In order to include the most relevant papers, manuscripts are shortlisted as per the following criteria-

1. The paper must be in English language only.
2. The paper must come within the purview of the selected field.
3. Paper is easily accessible from digital library.
4. The year of publication of the paper lies between 2003 and 2021.

Some exclusion criteria have also been applied after the initial search of the papers. Manuscripts are excluded as per following criteria

1. Thesis
2. Patents
3. Research articles which do not lie within the said duration.
4. Research question is inapplicable to the research papers.
5. Duplicate papers appeared in the search are eliminated to conclude reliable result.

2.2 Subservient Level

The articles that fulfill the requirements of research question are finally shortlisted at inceptive level. Fact finding are conducted from the shortlisted research papers based upon the research question. Considering these points, research papers of the years between 2003-2021 are used in the selection process. 131 research papers are included in the review which satisfies the paper selection criteria. Key agreement schemes in WBAN are focused to provide extensive review of different key agreement schemes and highlight their key aspects and discuss their limitations and challenges.

3 Difference between WSN and WBAN

Wireless Sensor Network (WSN) and Wireless Body Area Network (WBAN) have been treated closely by some of the authors but there are considerable differences between both the environments. Some major differences in WSN and WBAN are found worthy to be discussed[24]. WBAN is spread around human body within a range of few centimeters/meters whereas in case of WSN, it is extended up to few kilometers. To improve the robustness and longevity of the system, many redundant nodes exist in WSN but this sort of arrangement is not feasible in WBAN as it would increase the temperature of body and harm the tissues in case of invasive bio sensors. Frequent node and battery replacement in WBAN environment is not easy as the sensors are sometimes implanted inside the body; on the contrary WSN environment supports easy node and battery replacement. WSN is established over a large geographical area using multi hop routing. No routing is required in one-to-one connection between sensors and personal server or there requires two to three hop connections at the max in case of WBAN. WSN follow a consistent network topology over a period of time whereas the network topology in WBAN is dynamic in nature due to movement, different posture and gait of human beings. The propagation of electromagnetic signals through the human body is variable due to the differences in the body formation or thickness of individuals and subject to absorption and reflections within the body. These waves diffract around the human body rather than passing through it. Additionally, individuals' mobility and posture also affects the efficient packet delivery. As a whole, the environment of WSN and WBAN is different in total. Consequently, the security requirements of WSN and WBAN are also different.

Table 2. Differences between WBAN and WSN

Attribute	WSN	WBAN
Scaling	Large (may be 1000 nodes)	Small (may not exceed 20 nodes)
Operational Area	Up to few kilometers	Within a range of few centimeters/meters of human body
Battery replacement	Easy	Not feasible in case of invasive bio sensors
Redundant nodes	Plenty of redundant nodes may be accommodated for better connectivity	Not feasible in invasive sensors, unnecessary burden on human body in wearable sensors
Network Topology	Consistent over a period of time	Dynamic in nature due to movement, different posture and gait of human beings
Routing	Multi hop routing occurs	No routing is required in one to one connection of sensors with personal server or two hop connection at the max
Human Intervention	Not feasible	Possible rather necessary in case of emergency
Security 1. Message Integrity 2. Node Authentication 3. Prevention from eavesdropping 4. Prevention from routing attacks	1. Necessary 2. Necessary 3. Necessary 4. Necessary	1. Necessary 2. Necessary 3. Necessary 4. Not always

4 IEEE 802.15.6

IEEE 802.15 Task Group 6 was created in November 2007 to develop the standards of WBAN[25]. Its objective was to design communication standards and protocols optimized for low power bio-sensor devices which are employed in or around human body. The first version of IEEE 802.15.6 was published in 2012. As per the standards, maximum data transfer rate is 2 Mbps within the proximity of .01 to 2 meters and power consumption range is 1 to 10mWatt. Different countries follow different frequency band specifications. WBAN works within the frequency bands of 400 MHz (402-405 MHz, 420-450 MHz), 800 MHz (863-870 MHz), 900 MHz (902-928 MHz, 950-956 MHz), and 2.4 GHz (2360 MHz-2400 MHz, 2400-2483.5 MHz).

These standards talk about Physical layer, Medium Access layer (MAC), frequency bands of operation, frame format and security specification of the WBAN standard. However, Toorani in[26] provide an analysis of proposed standards and found vulnerabilities in them.

5 Attacks on BAN

This section talk about several possible attacks on BAN.

1. **Eavesdropping Attack**[27]: Eavesdropping is a serious threat for all those systems which transmit their signals over the air. BAN is also not immune to this attack. Eavesdropping is a passive listening but the knowledge gained by this attack is utilized to launch other active attacks.
2. **Message Corruption**[28,29] : Message Corruption is one of active attack based on eavesdropping which capture the information first, modify and reintroduce in transmission again. The modified information gives false impression to the Doctors and Caregivers about the actual health of the patient. It may be fatal for a human life in case actuator is attached with the patient's body and Doctor initiates a dose remotely based upon the information received.
3. **Impersonation or Node Cloning Attack**[28,30]: Another focus area is trust of a node. The compromised information gathered using some other attacks, impersonation of a legitimate node is performed. The attacker may launch attack to steal the information in real time through this node.
4. **Replay Attack**[29,31] : An attacker with a malicious intent can capture a message, replay it at a later time with or without changing its contents. Such bogus messages are induced into the network to drain the energy of the system. It may also lead to take wrong decisions.
5. **Forge Base Station Attack**[30] : In wireless environment it is possible to create forge base station which make enable to collect data from legal sensor node.
6. **Man in the Middle Attack**[31] : MITM attack is a powerful real time attack, where the attacker is sitting between two parties and communicates to both ends concealing her identity.
7. **Guessing Attack**[31]: Passwords may be guessed which it is required to log into the system. Online guessing or Offline guessing are the two ways by which possible passwords may be guessed.
8. **Reflection Attack**[32] : An attacker can launch reflection attack by manipulating the challenge handshake mechanism of Authentication protocol. Attacker can gain unauthorized access to the system without having genuine credentials.
9. **Denial of Service Attack**[29,33] : The aim of the Denial of Service (DOS) attack is to bar the accessibility of the system through network resources. The target is flooded by sending a large number of fake packets in order to consume the communication bandwidth and computing capabilities. It is really difficult to manage DOS attack in resource constraint environment of BAN.
10. **Tracking Attack**[34] : Attacker can eavesdrop and able to identify the identity of the person by determining the actual source of BAN communication.
11. **Matching Attack**[34]: When the message is small in size as in case of WBAN, attacker generates a pool of public keys. She tries to decrypt the message content by applying different key values and find the meaningful values.
12. **Collusion Attack**[35] : An attacker acquires the key material for few nodes and crypt-analyzes the keys for other nodes of the network. The required starting stuff can be gathered either by conspire or using an access to multiple compromised nodes.
13. **Key Compromise Impersonation Attack**[36] : Crypt-analyzes the private key of any node may lead to impersonation attack.

Hello flood attack, selective forwarding, wormhole attack, sinkhole attack and sybil attack are all routing based attacks which are more relevant for WSN. These attacks are not very potent in WBAN because the nodes may be connected using single hop which does not require any type of routing.

6 Security Requirements of WBAN

There are certain expectations from WBAN from the security perspective without which the crucial medical data would not be secure. Based upon the literature review, following are the expectations of WBAN from security perspective.

1. **Data confidentiality** [37] : Medical data is private and crucial in nature which needs to be protected from unauthorized access. Data confidentiality in transmission as well as in storage requires being secured by means of cryptographic techniques.
2. **Node authenticity** [37]: Node authentication is a major concern in WBAN. Spoofed nodes may ruin the entire network authenticity. Lightweight cryptographic methods are required as traditional techniques are not suitable for energy constraint resources.
3. **Data integrity** [37]: Personal health related data may be modified in transit in absence of any mechanism to ensure the data integrity. It could be dangerous in life critical situations. System must ensure to detect any modification in data. To check the data integrity, lightweight cryptographic hash functions are required which can authenticate inter BAN communication.
4. **Mutual authentication** [38] : The nodes of WBAN participating in the system must authenticate one another to thwart Man-In-The-Middle (MITM) attack.
5. **Unforgeability** [39] : A secure WBAN must ensure that the personal server cannot be forged. A compromised server may divert all the medical data towards the attacker which can play disastrous to the system.
6. **Unlinkability** [31] : Unlinkability is ensured if the system is able to hide the identity of sender and the corresponding receiver. The identity of the sender and receiver must be hidden during communication.
7. **Forward secrecy and backward secrecy** [40] : In backward secrecy, when a node joins a network after it was established, system must not provide the access of those messages exchanged earlier before it joined the network. In forward secrecy, a node which has left the network is not allowed to access the messages exchanged after its departure.
8. **Scalability** [40] : System must ensure the implementation of security schemes keeping in view of the scalability of the system. It must support the inclusion of more nodes without causing any security flaw.
9. **Freshness** [41] : To maintain the freshness of data packets, time-stamping on the data packets is done. It will identify the new and old data packets. It will help the system to thwart the replay attack.
10. **Prevention of DoS attack**: Denial of Service attack is meant to forbid the accessibility of any service or resource to its intended users. It is accomplished by flooding the target resource that triggers a crash.
11. **Prevention of Node Capture attack:** An adversary can capture the node and install malicious software. It is redeployed to launch various attacks.

7 Key Agreement in WBAN

The first and foremost agenda in securing WBAN is key agreement schemes. To successfully establish a secure network, the keys are negotiated upon all the nodes participating in the network. Key agreement is a mechanism in which sensor nodes authenticate one another by sharing secret keys among them. The basic steps involved in key agreement process is as follows [42]

1. **Key Generation:** Either the agreement keys are pre-deployed or calculated dynamically at run time using biometric or RSSI values.
2. **Key Agreement:** After key generation process, sensor nodes authenticate one another to create WBAN.
3. **Key Refreshment:** All the keys are timely refreshed to prevent any type of cryptanalysis attack.
4. **Key Revocation:** It refers to the process of withdrawing the cryptographic keys of the nodes known to be compromised.

Traditional cryptographic methods are categorized in two categories namely symmetric key and asymmetric key methods. A symmetric key method is easy to integrate with less memory requirement as well as it is fast to execute. Symmetric key method is preferred in general but sharing a common key to both the ends is always a challenge. Different mechanisms of sharing the key between the parties have been proposed by the researchers from time to time. An asymmetric key method of encryption and decryption is slower and would seek more energy and memory requirement which makes it unsuitable in resource constraint environment of WBAN.

The nodes of WBAN are required to be authenticated before the network is established. Secret keys must be distributed to all the nodes of the network securely. The key agreement schemes are classified as physiological value based, non-physiological

value based and hybrid key agreement schemes by Ali and Khan[29]. However M.Kompara and M Holbl[19] have classified the key agreement schemes into four classes namely traditional, physiological value based, hybrid and signal based secret key agreement schemes. The approach used by[29]and[19] is same with one exception. The non- physiological value based scheme of[29]is divided in two categories as traditional and signal based secret key agreement by[19] considering both the schemes are fundamentally different.

Pre-distributed keys are pre-installed before the network is established in traditional key agreement schemes. The advantage of this scheme is that the execution time processing efforts in calculating the keys are less but it requires additional storage space to store the keys. Biological parameters are used to compute the common secret key in physiological based key scheme. As same biometric parameters are used to calculate secret key at all the deployed nodes; the corresponding key values at all the nodes are expected to be the same. Hybrid key scheme is an amalgamation of both traditional and physiological values based schemes. The combination of two approaches produces better results. The fourth scheme i.e. signal based secret key generation scheme; is analogous to physiological values based key agreement. This scheme uses the characteristics of transmission channel and the biometric parameters of human body to generate key values.

7.1 Traditional key agreement schemes

Security keys are pre-deployed in traditional key agreement schemes. The advantage of this scheme is that the computation is not required to calculate the security keys whereas the memory requirement to store the keys is a major disadvantage of the scheme.

Initial idea of Deterministic Pair-wise Key Pre-distribution scheme (DPKPS) is suggested in[43]. Combinational design theory is used to pre-distribute key material to the sensor nodes as bivariate polynomial in the form of Blundo's polynomial. The method has shown perfect connectivity and provide resiliency for BAN in the presence of attackers as explained in[44]. Pair wise key distribution in DPKPS consists of two phases. In the first phase called initial configuration phase, the IT administrator of hospital authenticate all the sensor nodes and pre-deploy DPKPS key material in secured environment of hospital where intruders cannot invade. DPKPS material is unique for each sensor node and composed of n+1 discrete univariate polynomial of order λ. The DPKPS material create pair wise key in the second phase called as usage phase. The generation of key material is a two step process. Step 1: Choose n+1 bivariate polynomials (BP) combinatorially from a pool of n^2+n+1 BPs which are randomly generated. Step 2: Chosen n+1 BPs are evaluated at distinct points of a field. The polynomials and the calculated points in step 2 are used to generate pair wise key between the devices.

A bidirectional secrecy & collusion resilience key management scheme namely Forward Security (FoS) and Backward Security (BaS) i.e. FosBaS was introduced in[45]. It is a mechanism to deploy a shared group key in BAN. This scheme is based on the concept of Chinese Remainder Theorem (CRT). There are multiple BANs connected to one server. Each sensor node of a BAN holds a unique ID (S_i). In initialization phase each individual sensor of every possible BAN obtains a unique prime number K_i as a key from the server. Server maintains a combination of sensor id & corresponding key in database. To form a group G_k, health personal selects few sensors & collect their corresponding IDs {S_i, …. S_j}and calculate Offset Code Book (OCB). This information is sent to server along with Message Authentication Code (MAC). Based upon the encoded IDs, server finds the corresponding keys (K_k). K_k is used to compute a broadcast value x using CRT. This x value is communicated back to sensors and used to compute new group key. The key is updated as and when any sensor is excluded from the group due to medical or technical reason. Nodes may be added into or removed from the group anytime. FoS ensures the communication held earlier must not be accessible to recently inducted sensor. BaS ensures that if any sensor leaves the group any time, it cannot access the future communication. FoSBaS ensures a bidirectional security sensor association for group key management using Chinese Remainder Theorem.

An efficient lightweight method for distributed security key mechanism named Multidimensional α Secure Key Establishment (MαSKE) is proposed in[46] which is based on polynomial α secure system. There is a central authority called MSN administrator who manages the registration process of sensor nodes including key material distribution, key update and revocation. A sensor node stores a cryptographic key material (KM), a lightweight digital certificate (LDC) and a security policy (SP). In the set up phase trust center (TC) coordinates the deployment of KM, LDC, and security policies to sensor nodes. Security handshakes and access control is managed automatically using this key material in the next phase without any involvement of TC. TC is required in case of updation or revocation of key. αSKE is a key distribution system which ensures that α-entities are required to be compromised to crack the system. Initial key establishment and access control role verification process use polynomial based α secure system which is stored at a secure location at the trust center. It uses symmetric bivariate polynomial of degree α over a finite field to generate & share the key material to each sensor node. MαSKE distribute multiple uncorrelated and independent sets to sensor nodes. The ID of a sensor node is generated using LDC by calculating hash of all its attributes. MαSKE and LDCs provide three different methods namely Cryptographically Enforced Access Control (CEAC),

Role Based Access Control (RBAC) and Identity Based Access Control (IBAC) and make the key generation & access control very efficient and fast.

In another traditional scheme Low Energy, Secure and Flexible Communication Protocol (LEXCOMM)[47], every sensor node uses a pre-deployed key for the first time when system is started otherwise temporary key is generated in rest of the cases. The coordinator of network broadcast a beacon packet for synchronization of network. The beacon packet consists of five parts: message, TDMA period, rest period, CSMA period and next beacon message. Every sensor node has been assigned a priority number. The priority number determines that which node has more rights to transmit in case of channel noise. Whenever any node joins the network, the coordinator makes an entry into the database about its node ID, its priority number together with other details like the amount of data to be transmitted, frequency of data transmission and time slot requirement. When everything goes fine, the coordinator allocates the requested slots to all the nodes. In case of slots deficiency, the coordinating node apply deficiency distribution algorithm in which available slots are allocated as per priority of individual node. The contention period may be used by the sensor nodes for re-negotiate its service terms with the coordinator nodes. CSMA period is positioned before the beacon message due to the same reason. Protocol uses acknowledgement at application layer or link layer. It may also use no acknowledgement policy depending upon the type of node. A proper retransmission process is followed in case no communication is received from sensor nodes. Transmission Delay and Clock Drift is calculated by exchanging few messages at the time a node is joining the network. All the nodes must follow a synchronization procedure at the time of joining. A lightweight version of AES is used for data encryption. Energy consumption is restricted by applying strict sleep awake schedule for the nodes.

Selimis et al.[48] categorized the transmitted data into sensor data and control data. Sensor nodes send its data to master node in unicast fashion whereas the master node broadcast control messages back to sensor nodes. Two types of keys are considered in symmetric key cryptographic primitives. A node key is a common key between a sensor node and server. Network key is shared by all nodes in the network. The core protocol consists of three phases. In node key pre-loading a unique key is installed in each sensor node in advance. The second phase of the process is network discovery phase in which a sensor node join the network after key agreement. In last phase all the nodes share the common key after network key update.

According to Efficient-Strong Authentication Protocol (E-SAP)[41], device is registered by Hospital registration desk and provides a secret key to the devices. Healthcare professional is authenticated using two-factor authentication which includes password and smartcard. Patients are also registered at registration center of hospital and corresponding ID and sensor kit's information is sent to concerned healthcare professional to enable him to access the data from the sensor kit. Healthcare professional sends a login request to patient's node. User is authenticated and a secure session key is generated and shared to exchange the data between sensor node and healthcare professional. There is an option for the user to change the password as well. He et al.[49] found some of the vulnerabilities in E-SAP scheme and proposed their own scheme to rectify the flaws.

Two group device pairing schemes were introduced in[50] and[51] which use light signals for initial exchange. Group Device Pairing (GDP) based Secure Sensor Association and Key Management is a unique way of group key agreement for a batch of ten nodes using LED blinking sequences which can be done within 30 seconds. It consists of three phases. In pre-deployment phase, new nodes are procured and group key is calculated. Keying material (KM) is distributed among all the nodes using group key. In deployment phase, nodes are deployed and pair wise keys are computed after creating BAN. In working phase; along with all the normal functions of data exchange, keys are periodically updated. New nodes may join or leave the network and revocation may also be done. Light channel for sensor Initialization and Radio channel for Authentication (LIRA) is a multichannel key deployment scheme which uses a visible light channel to exchange secret keys to the node. Light signals are easy to block so that the attacker cannot intercept them. Sensors with light detectors are required for this purpose.

In a resource constraint environment of WBAN, computation and storage is a concern in implementing asymmetric encryption. RSA based traditional asymmetric encryption would not be appropriate due to memory and processing power constraints[52]. Several traces of asymmetric encryption along with ECC are found in different works[53]. ECC provides better security than RSA and Elgamal with smaller key. ECC is also beneficial in constrained environment like BANs[54,55]. Wang et al.[34] introduce HIGDCP which provide security using a combination of ECC and human interaction. Amin et al.[40] have used Elliptic Curve Cryptography (ECC) together with pre-deployed private and public keys. These keys are used to generate the session key for symmetric encryption. ID-based Elliptic Curve Diffie Hellman key exchange protocol is used in[56]. Huang et al.[57] introduced Elliptic Curve Diffie Hellman version of Symmetric Hash commitment Before Knowledge Protocol. Dynamic distribution of keys is performed rather than pre deployment of the keys.

[58] provides four schemes for authentication and key agreements. All schemes use ECC for key agreement. The first scheme is a basic scheme which is an unauthentic key agreement scheme. Hidden public key transfer protocol is the second authentication scheme. A segregated protected channel is used to transfer the secret key. The password-authenticated key agreement protocol uses the password scrambled form to send the public key to other end which is retrieved with password information. In fourth

scheme named as display authentication; hidden nonce contained in witness value is sent in first message. The actual nonce is communicated in final message which can be compared with the nonce and witness values communicated in first message to ensure the integrity of the message.

[59] is an ECC based key management scheme to protect medical information in healthcare. The entire scheme is divided in three phases. In setup phase, Certification Authority chooses a elliptic curve and perform system initialization. Sensors are used to create WBAN. WBAN controller or Smartphone acts as sink node. In registration phase, the data sink uses its registration id i.e. sim-card number and public key to register with CA. CA generates key material which is exchanged with the other party in verification and key exchange phase. Consequently, session key is generated.

[60] is ECC and hash chains based key management protocol. A PC (patient controller) such as PDA or smart phone collects the values from all the sensors of the body. ECC is used to calculate a shared secret key between PC and each sensor node with the help of LED blinking pattern. Synchronized blinking pattern ensures the successful establishment of WBAN. ECC is found to be more efficient than RSA. Group key is always computed by PC as it has sufficient resources. It is distributed to all the nodes using shared secret keys. Hash chains are used to ensure authentication. Hospital itself is key generation centre (KGC) which choose a random integer as its private key and computes the corresponding public key.

Some researchers have also used Boneh-Franklin's Identity Based Encryption Algorithm (IBE) in different ways to calculate the keys. The idea of IBE is based on Asymmetric Key Cryptography. IBE does not generate the combination of public key and private key similar to RSA. The data is stored at central server. The keys in IBE is based upon the identity of the doctor who wants to access the data, date and time on which he/she is willing to access the data. IBE generates the public key for 1 hour duration from a string = {date/time/ER}. The ER is the identity of the doctor whereas date and time parameters are as usual. The corresponding private key is generated later. A variation of the method, IBE-Lite[34,60] which is lightweight IBE, retains the attribute of conventional IBE and can be applied on sensor node. It is based upon Elliptic Curve Cryptography (ECC). Public key is independently generated by a sensor using an arbitrary string. Data is encrypted using the key and stored to the remote server. Whenever a doctor wants to access the data, the administrator will generate the same key using same string and provide access to doctor. Huang et al.[27] extended the idea of IBE-Lite further.

A lightweight protocol providing anonymous mutual authentication was proposed by Li et al.[61] who claimed the protocol to be secured against various types of attacks. In cryptanalysis of Li's protocol Chien- Ming Chen et al.[62] have found that the protocol is vulnerable against three types of attacks i.e. offline identity guessing attack, hub node spoofing attack and impersonation attack on sensor node. A secure mechanism addressing these problems with similar efficiency is proposed in[62].

A secured Energy Efficient Mutual Authentication and Key Agreement Scheme for Wireless Body Area Networks (SEEMAKA) is proposed by Narwal B et al in[63]. SEEMAKA uses fewer hash functions and bitwise XOR operations. The algorithm is analyzed using informal analysis as well as tested using AVISPA tool. The performance of SEEMAKA is compared with other methods using NS-2 simulator. Two XOR operations are reduced at master node and makes the master node as well as the sensor node safe from spoofing attack.

Ali et al.[64] have designed an attribute based encryption (ABE) scheme with lightweight encryption and decryption mechanisms. Contrary to other schemes which use heavy computation in their encryption process, the scheme proposed by Ali et al. uses very few computations to encrypt the data at the tiny sensors. This scheme also reduces the communication overhead as partial cipher text rather than the complete and larger size cipher text is sent to cloud server which is a usual phenomenon in other schemes.

Singh U et al.[65] proposed a novel authentication scheme for WBAN with anonymity. This scheme is certificate-less and lightweight. The scheme has three phases namely initialization, registration and authentication phase. It uses public and private key system in initialization phase as well as registration phase. The scheme uses a random parameter for the communication which ensures anonymous unlinkable session. Time stamps are used to check the freshness of the message which helps to thwart the replay attack. The scheme also provides forward/backward secrecy, confidentiality, authentication and resilience to forgery etc.

Mo J et al.[66] proposed two factor authentication and key agreement scheme for WBAN which is an improvement of the two-factor authentication protocol based on quadratic residues with fuzzy verifier presented in[67]. The proposed algorithm[67] is cryptanalysed & is found that it is not immune to Known Session Special Temporary Information (KSSTI), DOS and privileged insider attack. The improved scheme is analyzed under random oracle model and demonstrated that the method is secure and efficient against different known attacks. A comparison with other scheme is also demonstrated.

A hybrid Advanced Encryption scheme for a protected wireless sensor data in secure transition and storage is proposed in[68]. The purpose of the proposed scheme is twofold. Effective key pairing mechanism using modified RSA algorithm and authenticated access of the user by modified AES algorithm is ensured. This scheme uses the combination of symmetric and asymmetric encryption technique for key pairing mechanism as well as for security. The proposed scheme is compared with

other existing algorithms on several parameters and found its performance better than other existing methods.

An efficient Lightweight Key Agreement and Authentication Scheme for WBAN is proposed in [69]. The scheme is an effort to overcome the security gaps particularly base station compromise attack and sensor node impersonation attack found in the method proposed by M. Kompara et al. [70]. This scheme is also compared with other related schemes. The scheme has been kept lightweight and is verified using AVISPA tool. The scheme is lightweight in terms of storage, communication, computation cost and time.

Secure new node ID assignment for internet integrated wireless body area networks is proposed in [71]. It is a scheme using public key cryptography to assign a new node ID for newly join node to create WBAN. The authors performed design, energy and computation cost analysis of the proposed algorithm.

A lightweight key agreement scheme in WBAN is proposed in [72]. The protocol has used less number of hash functions and XOR operations to keep it lightweight. Informal security analysis of the proposed scheme is conducted for the well known attacks like eavesdropping attack, anonymous and untraceable sessions, sensor node capture attack, replay attack and forward/backward security. Performance analysis for storage, computation and communication cost is also conducted for the proposed algorithm.

Shen et al. [59,73] introduced a key management protocol which exchange keys between the personal server and sensor node at one end. On the other end it exchanges keys between the personal server and medical professional. Hash chains are used to achieve authentication.

TinyZKP [30] is a Zero Knowledge Proof (ZKP) based scheme. In this scheme, personal server (verifier) authenticates the sensor nodes (prover) using the knowledge based upon the secrets it stores without actually revealing these secrets to server. The secrets may be some crucial information received from prover. In the first phase secret and public keys of sensor nodes and server are generated. In authentication phase each sensor node proves itself to base station using zero knowledge proof.

Ibrahim et al. [74] proposed a scheme in which parameters are pre deployed in personal servers and sensor nodes by the system administrator. One of the parameter is a temporary id for each of the node. A corresponding parameter related to temporary id of each of the node is available with personal server. Nodes are authenticated by this combination available at personal server. It prevents the attempt to join the network later by any foreign node.

M. Almuhaideb et al. [75] provides two protocols P-I and P-II for authentication and re-authentication respectively. The scheme is implemented in four phases (i) initialization and registration (ii) authentication (iii) re-authentication and (iv) expired key deletion. The scheme offers a better key management and uses high randomness to improve the security parameters.

Song Y. et al. [76] proposed a method consisting of two subsections. In the first section, mutual authentication of PC to sensor and in second subsection a group key generation between sensors is performed. The scheme follows security properties and contribute resistance to well known attacks.

7.2 Physiological value based key agreement schemes

Physiological signals or bio-signals may be used to calculate the symmetric keys at sensor nodes. All the sensor nodes of WBAN accesses a uniform physiological value independently and calculate the symmetric keys accordingly. These symmetric keys are utilized in encryption and decryption processes performed at the nodes. These parameters vary from one human being to another as these values are unique to an individual [37]. It would a better idea to generate key values at every sensor node independently as the exchange of data is most energy consuming process in WBAN. This method of key generation is energy effective as it requires less energy in secret key calculation rather than the energy consumption required to exchange the data during other key agreement schemes. Keys are changing dynamically depending upon the physiological signals. Biometric signatures are distinctive to a human body which is a way ahead in Intra-BAN security [77]. Biometric signals such as Electrocardiogram (ECG or EKG) [78–80], Blood Pressure (BP), photoplethysmogram (PPG) [78,81–83], Blood Oxygen Level (SPO_2) etc. may be used for this purpose. Inter-pulse interval (IPI) is also used to compute the symmetric key [84]. IPI is the time gap between two successive pulses and compatible to use with ECG and PPG signals.

Physiological value based key methods are divided in two categories on the basis of key distribution policies [77].

1. Physiological value based protocols with pre-distributed secret keys
2. Physiological value based protocols without pre-distributed secret keys

Other authors [29] have categorized physiological value based protocols with pre-deployed secret keys as hybrid solutions because these schemes borrow their methods from traditional & physiological based scheme. Physiological value based protocols are divided into fuzzy and non fuzzy groups [29]. Further there are several fuzzy protocols without pre-distributed secrets. Protocols with fuzzy vault (e.g. PPG based key agreement (PKA) [82,83], Ordered Physiological Feature Based

Key Agreement (OPFKA)[85], Protocols with fuzzy vault and encoded features (Physiological signal based key agreement (PSKA)[86], Protocols with fuzzy vault and encoded key materials[87], Fuzzy vault with a cubic spline curve[88] are the examples of fuzzy protocols without pre-distributed secrets.

Ordered Physiological Feature Based Key Agreement for WBAN[85] is a novel way of key agreement between two nodes which is based upon physiological signal features. The same physiological signal (ECG, PPG or BP) read by distinguished sensors at different parts (chest, fingertips or limbs) of body have overlap values but with some gap. OPFKA is an efficient protocol which transfers the secret features of one sensor to another in such a way that the sensors are able to identify their overlapping features. First of all, a feature vector is prepared by each sensor and sent to the receiver. Feature vector may contain noise. Receiver generates a symmetric key based upon common feature. It returns the indices of matching features back to sender along with MAC of the key. The sender calculates its symmetric key using those values of features vector which are corresponding to the indices received from receiver.

A physiological feature based key agreement for WBAN[86] is a biometric parameters based system. The biometric parameters are of two types: static and dynamic. Fingerprints, retina and iris patterns are static parameters whereas ECG, IPI, PPG etc. are dynamic biometric parameters due to their randomness and time-variance behavior. PFKA calculates and distribute the symmetric key which is based upon the features extracted from Electrocardiogram (ECG) signal. Either enhanced FFT or IPI method is used to generate features. In FFT, the sampling rate of biometric signal is same at two sensors. FFT is applied on the signals after dividing them into windows. Peak index and peak values of each of the overlapping window are calculated after applying peak-detection algorithm. Values are quantized and concatenated to form a feature vector (F). In IPI method, the last 4 bits are quantized for each IPI. The bits of three adjacent IPIs are concatenated after quantization to form a feature. These feature vectors are changed with a vector of random numbers along with its MAC. Reed Solomon coding is applied to form a modified vector which is exchanged between sensor and receiver.

[89] is a key agreement scheme based upon Linear Prediction of ECG features. The process is summarized in Figure 3[89]. It calculates symmetric keys based upon ECG signal features and use Linear Prediction Coding to compress the data before transmission. The transmitter node N_t and receiver node N_r want to establish a connection. The node N_t collects the N samples of ECG value for a fixed time duration of T_s. The features F_1 are extracted from the N-sampled set of values. F_1 is linearly predicted and produce the LPC coefficient vector (A) and the residual error of predicting F_1 (E). The value "A" is sent to receiver and value "E" is used to generate 128 bit session key using a key generation process. Entire key is not exchanged and only a partial value is sent across in terms of "A" value. BCH coding is used to adjust and correct the key K_1. Near similar method is used to generate 128 bit session key by receiving value "A" from sender.

Trust Key Management Scheme for WBAN[90] use ECG values to generate and distribute symmetric keys to sensors. Base station maintains a database of those keys which are shared with the sensor nodes. Base station has a pair of private and public key. WBAN architecture is divided into three layers. After the base station on the top, there is an intermediate layer of gateways. The nodes which are in close proximity are connected to one of the gateway. The protocol consists of four steps. In Key Generation phase, fiducial methods are used to calculate the interested area on a heartbeat. ECG values contain high degree of randomness and variance which is essential for good cryptographic keys. A symmetric key (Biokey) is generated after the feature extraction of ECG signals. Its morphed version after applying MD5 function is used as a session key ($K_{session}$=MD5 (Biokey). In second phase known as Key Setup phase; each node after calculating the $K_{session,}$ encrypt the Biokey using the public key of base station and transmit to base station. In third phase known as Key authentication phase; sensor nodes authenticate its gateway using a challenge response mechanism. In fourth phase called as Key Update phase, the keys are updated periodically to avoid long-term cryptanalysis. The key update process is initiated by the base station.

Yasmeen et al.[91] proposed an algorithm which is based on measuring the common ECG signals at the sender as well as recipient sensor. The algorithm is lightweight as it uses the information from the previous connections to calculate the new and random security key for the current sessions.

ESKE[92] is ECG parameter and fuzzy commitment based protocol. The fuzzy commitment in ESKE ensures that the protocol can tolerate noise and randomness in ECG signals. The combination of ECG signals along with fuzzy commitment is used to create confusion between correct point sets and chaff points. In fuzzy commitment scheme, the biometric values close to the original can be accepted using the idea of hamming distance. Central Unit (CU) observes biometric values and sends to a sensor along with some chaff points. The sensor compares the received values with the biometric parameters observed directly. If sufficient number of point match; sensor is approved and a session key is established. Because of uniqueness, biometric parameters can be used to calculate the cryptographic key dynamically. These keys are further encrypted to provide security to biometric driven cryptographic keys.

Broadcast –Based Key Agreement Scheme Using Set Reconciliation for WBAN[79]. A node share a common key with personal server which is generated using feature set extracted from ECG. This scheme uses the idea of set reconciliation. If

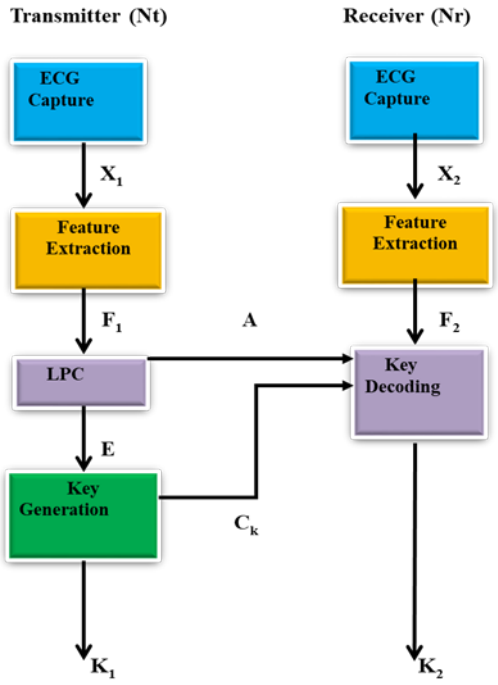

Fig 3. Key Agreement Scheme Based Upon Linear Prediction

A={1,2,3,4,5,6,8,10} and B={1,2,4,5,6,8,9} are two sets. The reconciled set contains the elements of A and B and missing elements of both the sets. The difference in both the sets is eliminated by minimal exchange of information. Two different hosts extract the features from ECG values and adjust the difference in their values using the same method used in set reconciliation method. PS broadcasts minimal information related to feature set to all the nodes. After applying the reconciliation process each node calculate the symmetric key to be used for data exchange.

Electrocardiogram (EKG) based key agreement scheme[93], generate a common key at two sensor nodes in plug and play manner without requiring any kind of pre-deployment. The design goals of a symmetric keys like randomness, time variance and sufficient long length are met in EKG based key agreement scheme. The values of EKG signals measured at two distinctive sensors are different but the trends are similar. Sampling is performed at 125 Hz and a particular interval of 5 seconds. Frequency component is removed from the samples as it does not affect much to the overall power of the signal. Samples taken over five seconds are divided into five parts and FFT is applied on each of these parts. Feature vector (F) is created from FFT coefficients. Filtering is performed to remove the higher level of entropy in quantization process. Feature vectors are exchanged between nodes and symmetric keys are calculated.

An improvement of[93] is proposed in An Improved EKG-Based Key Agreement Scheme for BAN in[94], which uses discrete wavelet transform (DWT) for feature extraction rather than FFT as performed in[93]. The computational cost using DWT is found to be linear.

Plethysmogram based Secure Inter-Sensor Communication in BAN[82] use photoplethysmogram (PPG) signal to calculate feature generation. Pulse oximeter is used to measure PPG. Frequency domain analysis of PPG signals are performed to generate the features as frequency components of physiological signals produce same values irrespective of the fact that at which part of the body they are measured. Time domain analysis performed on the values of two PPG signals measured at two distinctive sensors showed that the sensor values are different but the trends are similar. Sampling is performed at 60 Hz and a particular interval of 12.8 seconds which produces 768 samples. FFT is applied in each of the five overlapping windows acquired after sampling. Peaks are identified using peak-detection algorithm. <Peak index, Peak value> pairs are quantized and concatenated to form a feature. Features measured from different samples constitute feature vectors. Random symmetric key is generated at one of the sensor and hidden using feature vector. The hidden key is communicated to other sensor. The receiver unlocks the symmetric key using its own feature vector. To compensate the difference between the feature vectors of sender and receiver, fuzzy vault scheme is used.

Majority of physiological value based key agreement schemes are centered on fuzzy vaults[95]. In fuzzy vault scheme a polynomial is selected to lock a secret K. The coefficients of the polynomials hold the value of the secret. A common value is chosen to lock the vault. Physiological values (PVs) are those values which are common and shared between two parties. These PVs represent the X coordinate and are used to calculate the corresponding Y coordinate using the selected polynomial. To secure the previously created points, other points called chaff points are also included which are selected randomly. The result is a fuzzy vault. The fuzzy vault along with a hash value H(K) is sent to other entity. PVs i.e. X-coordinate are gathered independently by other entity. Polynomial function is reconstructed by finding the appropriate points in the vault. Secret is assembled and hash H(K') is calculated. The values of H(K) and H(K') are compared.

The other works which follows the non-fuzzy approach are protocols with multiple commitments[96], protocols with matrices comparison[93,94] and protocols with Reed Solomon decoding[93,97]. However, it is analyzed that non-fuzzy solutions are not very common.

Physiological value based key agreement scheme offers following advantages[98]-

1. Keys are generated at run time eliminating the requirement of pre-deployment of keys in WBAN nodes. It would allow the network to work in plug and play environment.
2. The time taken in setting up the initial environment would come down.
3. Space requirement would be reduced.
4. As keys are not fixed and generated at run time depending upon the physiological values, network restructuring would not be an issue.

Physiological based key agreement schemes experience following challenges in key negotiations-

Lightweight computational design [77] In physiological value based scheme, the storage requirement comes down comparatively to other schemes but computing requirement increases which would put more strain on the battery life of the node.

Signal Obtrusion Two BAN users in close proximity can interfere each other's network which can lead to the false calculation of the keys based upon physiological parameters[77] .

Variation in physiological signals[77] There could be variation in the signals measured at two different nodes of WBAN due to the high entropy of the signals which propagate to calculation of false key values.

Security Assurance[77] There should not be any access to the physiological signals to anybody who can get the benefit after calculating the secret key.

Proficient key generation[77] The physiological signals are varying randomly. The process of key generation must be fast enough to avert the variation in the key.

Noise Removal[77]Multiple sensors are located at different parts of the body. The signals may vary due to the positions of the sensors and nodes. The generated noise must be removed to calculate the exact measurement of the signal.

The challenge to implement the PVs based key generation scheme is the lack of randomness in physiological values. All the possible biological parameters namely BP, ECG, EKG, PPG, SPO_2 and IPI used to generate PVs have a short range which is contrary to the requirement of very large range and true randomness in the numbers used to generate symmetric keys at both the ends.

7.3 Signal Based Secret key generation schemes

Secret key generation schemes exploits the user specific signals to generate keys between two genuine nodes. These schemes are generally based on the signals which are easily available to all the sensors. However, to receive identical signal features at all nodes is always a challenge due to motion of human body and positioning of the nodes. The signals that show consistent values on different nodes are used to calculate the symmetric keys.

Generally protocols use two types of signals to generate the secret keys. A common property of a wireless channel or common physical environment is extracted to generate the keys. Received Signal Strength Indicator (RSSI) is most commonly used attribute of the wireless channel to compute the secret key at nodes. These signals are not possible to be reproduced outside the network as the same environment is hard to regenerate due to the positioning and dynamicity of the WBAN environment[99]. These values are highly dynamic in nature due to which replica generation is a challenge for an adversary.

Secret key generation schemes generally consist of four steps in these types of schemes-

1. Sampling Phase- The signal values of the mutual channel are measured by the communicating nodes.
2. Quantization- The analog values are quantized and symmetric keys are generated using digitized values.

3. Reconciliation or Noise Removal- The difference between the key values is removed and the two nodes agree on a common key.
4. Strengthening phase- During this phase, the key values are strengthen further to make the keys stronger and avoid the attacker to gain any information during the previous phase.

S.T. Ali et al.[100] presented a dynamic secret key generation scheme using temporal-spatial characteristics of wireless channel for BSN. The multi-path channel properties between two communicating sensor nodes are spatially unique. Authors verify experimentally that human body motion create channel variation in WBAN which helps to generate symmetric key at sensor nodes safely even in the presence of eavesdropper. The channel is sampled intensively for a brief period of time. The fast and slow components from the sampled signal are isolated using filters. Quantization is performed on both the signals independently. The base station and sensor node keep track of RSSI values. Noise is removed from these values and symmetric keys are generated. The eavesdropper measures a different channel and would not be able to generate the same symmetric key. The mismatch rate is high due to the motion causes fluctuations in the measurement of RSSI values in proposed scheme. The scheme was revised and mismatch rate was lowered in[101]. Later, they improvised their technique and further reduced the mismatch of the generated bits in[102].

Tsouri et al.[103] calculates symmetric key for BAN using wireless physical layer security (wpls) in presence of eavesdropper. RSSI values were measured at two nodes from the packets going back and forth. Proposed algorithm was used to generate the symmetric key on basis of the difference between consecutive RSSI values. After a fixed number of attempts, if the absolute total of all the differences is above a threshold number, a bit is generated otherwise the process is repeated.

Device authentication and secret key exchange are two major issues which are taken care separately. Authenticated Secret Key (ASK-BAN)[104] proposes a solution to both the problems simultaneously using heterogeneous characteristics of physical layer. The authentication of the devices is done using stable channels whereas the key generation uses relatively unstable channels. ASK-BAN authenticates on body sensors using trusted sensors as relay node. It uses transitivity in trust establishment among nodes. To establish secret key; ASK-BAN uses multi-hop paths which causes larger RSS fluctuations. Its extension Movement Aided Authenticated Secret Key (MASK-BAN)[13] is a dynamic channel based lightweight fast device authentication and secret key extraction scheme for WBAN which uses RSSI values for authentication and for building the keys.

Secure Authentication and Key Generation Protocol Based on Dual Antennas for WBAN (SeAK) scheme[105] uses the idea of dual antennas in BAN while the other protocols based on RSS use single antenna. The sampling can be performed by any one of the antenna present on device which provides great diversity. Authentication and secret key generation is done simultaneously in this scheme. This scheme generates a secret key of 128-bit in 640 ms as compared to 15.9 s in ASK-BAN.

One promising solution[106] for key agreement between two communicating parties is data reciprocity. It is an efficient method to extract a common key after removing the minor differences. The attenuation coefficient of RSSI value depends upon inter-node distance. RSSI values are also changed due to the movement of human body which alters the inter-node distance. The closeness of several sensors interfere the signals of one another. Probe messages are sent from node to PS and vice versa. The strength of RSSI values are measured at both ends which helps to calculate symmetric keys. It is purely a software based solution and does not require any special hardware.

According to[107] same characteristics of Physical layer are shared by two communicating parties in point to point channel. Keys are calculated on the basis of the received signal at any sensor node. Almost same value of the signal is measured at its peer node. The differences in the signal values are exchanged in terms of check symbols which help to compensate the gap in the values measured at two nodes. Error-correcting algorithm is used to regenerate the original data stored at other end. The method of exchanging the check bits rather than the actual data is found to be secure and significantly reduce the amount of information exchanged during key agreement process. Improved Juels and Sudan (IJS) algorithm is used in which the high order polynomial coefficient of RSSI is sent to other side. Reed-Solomon method is used to regenerate the signals from local RSSI and the received coefficients.

The joining of a new device in a wireless network is a three step process. Whenever a new device joins a wireless network; it's a three step process. New device first joins a wireless network (using common key). It then establishes communication with peer devices (using unique key). It finally connects to the cloud account (using copy and paste). Wanda- a 'magic wand' is a small hardware device shown in Figure 4[108] has two antennas. Both the antennas are separated by one-half wavelength. Wand calculates the difference in received signal strength measured by both antennas and determines the proximity with the device.

The two antennas in Wand device help to implement two operations: detect and impart which are essential to make new device part of the system. The device's proximity can be ascertained by observing the difference between the power readings of two antennas. Larger the difference, closer is the device. When the proximity of the other device is ascertained, it can use the reciprocity property of signal to impart information onto another device.

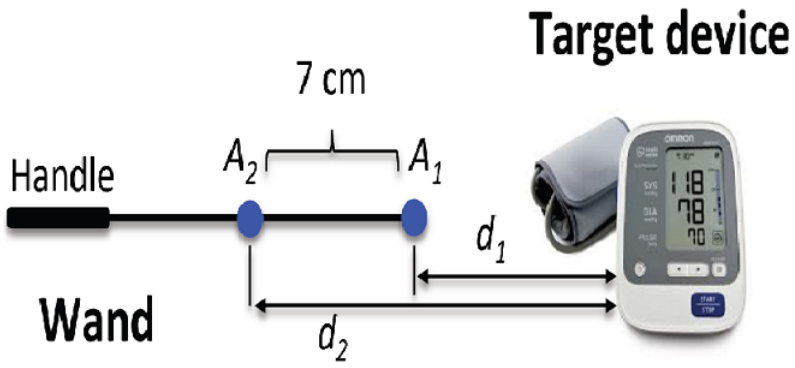

Fig 4. Wanda Mechanism

Low Mismatch Key Agreement Based on Wavelet-Transform Trend and Fuzzy Vault was introduced by Wu et al[109] to generate and share the secret key to other node even in the presence of eavesdropper. The sender node gathers RSSI value which is used to construct the fuzzy vault with a randomly generated secret key hidden inside it. The receiver extracts the key from the vault using highly correlated RSSI values.

The second group of schemes is based on some property of common physical environment exposed to both the nodes. Much work is focused on acceleration signals which are generated due to the acceleration of human body. Positioning of nodes on different parts of bodies pose a challenge as the different parts of body accelerates with different rate. The acceleration rate measured by the sensor placed on arm or leg is different than the sensors placed on chest or neck. Bichler et. al[110] presented a mechanism in which a secret key is generated by the acceleration data produced from shaking the device. A near similar method of shaking two mobile devices simultaneously was proposed by Mayrhofer and Gellersen[111]. Simultaneous shaking is an easy to use mechanism to pair two small mobile devices. The method based on common physical environment involves the same sequences as those based on wireless link characteristics.

Quach et al.[112] proposed a secret key generation mechanism which is dependent on ambient audio signals. Acceleration depends upon user's gait- the way that somebody walks. Measurement of acceleration on different parts of body is a challenge as different parts of body accelerates with different speeds. To compensate the gap between the readings of the sensors on arm and chest due to the different rate of acceleration, the acceleration due to the swing of arm has to be reduced[113,114].

Mubarak et al.[115] proposed a signal based protocol which is a two step scheme. In the first step of the scheme a compromise and impersonation attacks resistant (CIAK) authentication scheme based on Zero Knowledge Proof (ZKP) is proposed. In the second step a channel characteristic aware (CCA) authentication scheme based on ZKP is proposed. The efficacy of the scheme is more than 90% in comparison of other schemes.

7.4 Hybrid key agreement scheme

Hybrid key agreement scheme is amalgamation of physiological and pre-deployed key agreement schemes. Physiological values of an individual are unique and hard to recreate outside the network. To provide more robustness and security, pre-deployed keys are also taken together along with PVs to generate the secret keys.

Protocols with physiological certificate[116], protocols with multipoint key negotiation[117] and protocols with pre-distributed keys[118] are some of the protocols using hybrid key mechanism.

Secret Key Exchange Protocol (SKEP)[119] is an ECG based cubic spline interpolation technique to secure inter- sensor communication. All sensor nodes are preloaded with a number Nb. SKEP is a two step process: commitment phase and feature acknowledgement phase. ECG values are collected at nodes. The sampled values of ECG are divided into different windows. FFT is applied to each of the window. Feature vectors (F) are calculated from FFT coefficients. Sensor nodes uses RNGs to generate a vector F' of random numbers. Cubic spline method is applied on a combination of F and F' to generate coefficients vector (Coeff). BioScript = hash(Coeff) $\oplus Ks_{ession}$ is calculated. Encrypted value of BioScript, Coeff using the key hash (Nb) is sent to the receiver. As the receiver also has the number Nb, the received message can be decrypted.

BARI[120] is a hybrid key management scheme in WBAN which establishes a secure traffic from sensor node to the remote medical server through Personal Server. Each sensor node of the network is given a slot to change its key as per the key refreshment schedule issued by the Personal Server (PS). Three types of the keys are used to manage the whole BAN.

Communication key K_{comm} is maintained by PS and used to transfer the data securely through the network. Administrative key K_{admin} is used to refresh K_{comm} . Every node of WBAN contains its own key K_{bsc} which is also recorded by Medical Server (MS). In initial setup phase PS is deployed. K_{admin} and K_{comm} are preloaded with PS. Sensor nodes are preloaded with K_{admin} and K_{bsc}. These keys are used for initial establishment phase. Re-keying is done on the basis of biometric parameter in the next phase as per the schedule issued periodically by PS. All the keys are refreshed according to the circulated schedule. BARI+ [121] is a distributed key management scheme. BARI+ uses four types of keys. Apart from the three keys used in BARI, BARI+ uses an additional key $K_{SN,MS}$ which is a backup key shared between MS and sensor node.

A Biometric Method to Secure Telemedicine Systems [122] involves IPI values to create secure keys. Four types of keys are used in WBAN: K_{int} - predefined initial symmetric key, Key_{LPU} -symmetric key that shares between sensor node (SN) and Personal Server or Local Processing Unit (LPU), K_{server} - Key between LPU and Remote Server (RS), K_{phy} – Key between RS and Doctor or medical professional (PR).Session key can be generated using biometric parameters like heart rate variability, ECG and IPI. Keys are exchanged using MAC for secure transmission.

Secure and Efficient Key Exchange for Wireless Body Area Network (SEKEBAN) [123] uses electrocardiogram (ECG) to generate symmetric keys. There are some points of interest in heartbeat readings called fiducials. 67 consecutive IPI values generate 128 bits. It is also observed that the Hamming distances are less than 22 bits for the same person but in case of different persons the distances are of the order 80 bits or higher. ECG generated binary sequence contains sufficient randomness required to be a good symmetric key however a morphed version is used. MD5 hashing is used for morphing. The hashed data will not allow creating original data and serving confidentiality. The process of SEKBAN is summarized in Figure 5 [123] .

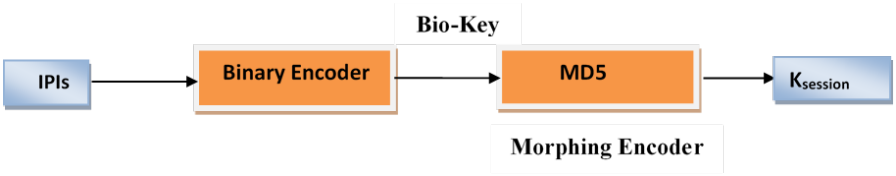

Fig 5. Session Key Generation in SEKBAN

IMDGuard [124] is a security mechanism for heart related Implantable Medical Devices (IMD). It remains operable even in case of emergency. It facilitates ECG-based key generation and an access control mechanism. Heavy security mechanism may lead to troubles in life critical situations. Security mechanism is switched off in emergency and an available doctor must be given access even if he/she is not authorized. The entire system is managed in two phases. IMD is implanted inside the body and an external device called Guardian is used as an interface between IMD and doctor. Guardian acts as a proxy server and performs all authentications on behalf of IMD. ECG values are used to share keys between IMD and Guardian. IMDGuard works in two modes: regular and emergency. In regular mode, Guardian would authenticate all communication. When Guardian is not detected by IMD; it enters into emergency mode and doctor may directly access to IMD.

IDKEYMAN [125] is a publisher-subscriber based key management scheme for WBAN. IBE is used to set up symmetric keys between publishers (sensor nodes) and subscribers (doctors or caregivers). There is no certification authority as available in traditional PKI rather a private key generator (PKG) generate private keys for nodes on providing their identification number as input. This method contains two phases. In publisher authentication model, publisher gathers the unique identification (PID) information of the user using RFID tags and validates the person before the actual communication begins. The second phase called identity based key management scheme operates in pre-operational, operational, post-operational and destroyed phases. In pre-operational phase, private keys and public keys of publishers and subscribers are pre-distributed. In operational phase, pair-wise session key is generated. In post-operational phase, the session keys are updated regularly. In destroyed phase, key regeneration process takes place in case of key compromise.

IAMKeys [126] generate random keys independently at both ends to encrypt each data frame. It eliminates key exchange requirement as keys are calculated independently at sender and receiver end. In secure environment, five dummy reference frames are loaded in WBAN Central Controller Node (WCC) and monitoring station data receiver. PRNG choose one of the data field from one of the reference frame as seed value and generate a random key. The data is encrypted using the key and transmitted. The receiver independently generates the key and decrypts the data frame. The encryption process include block and stream ciphers. It is also taken care that a single bit errors don't propagate and remain single bit error. In case of lost frame, a frame with latest values is sent to maintain the freshness of the data.

Sammoud et al. [127] proposed a biometric based symmetric key establishment method to exchange the data between two sensor nodes in WBAN. ECG signal is made available to all the sensor nodes and biometric based symmetric key is calculated

which is based on three entities. The protocol offers an optimal and robust security approach in WBAN environment.

In [128], a value of bivariate polynomial is pre-deployed. These values are used for key exchange. Hash values of PVs are X-Ored with pre-deployed keys to generate a random key.

8 Analysis of Key Agreement Scheme on the basis of different parameters

Tables 3, 4, 5 and 6 are prepared to show a comparison of different key agreement schemes of Traditional, Physiological, Signal based and Hybrid methods respectively on different parameters viz. data confidentiality, node authentication, data integration, mutual authentication, unforgeability, unlinkability, forward/backward secrecy, scalability, freshness, DoS attack, and Node capture attack as discussed in Section 6. Results of these comparisons are summarized and shown graphically using Figures 6, 7, 8 and 9. In figures, distinguished parameters are denoted on X-axis and the count of the algorithms following the corresponding parameter is denoted on Y-axis. Red color is used to denote the backward secrecy in Figures 6 and 9.

8.1 Analysis of Traditional Key Agreement Schemes

Table 3 is prepared to show a comparison of different Traditional key agreement schemes.

Thirty algorithms are studied in Traditional key agreement scheme. A summary of the study is shown in Figure 6.

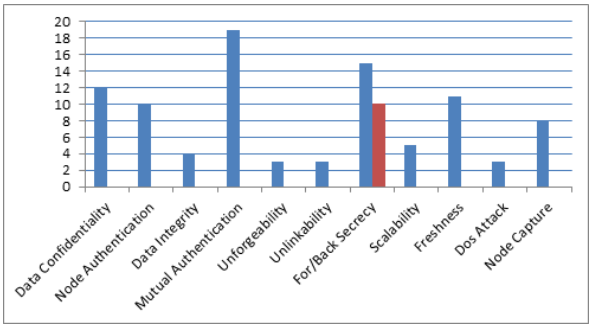

Fig 6. Analysis of Traditional Key Agreement Schemes

Maximum algorithms have considered the parameters like data confidentiality, node authentication, mutual authentication, forward/backward secrecy, freshness and node capture attack. The parameters like data integrity, unforgeability, unlinkability, scalability and DoS attack are less stressed upon.

8.2 Analysis of Physiological Key Agreement Schemes

Table 4 is prepared to show a comparison of Physiological key agreement schemes.

Nine algorithms are studied in Physiological value based key agreement scheme. A summary of the study is shown inFigure 7.

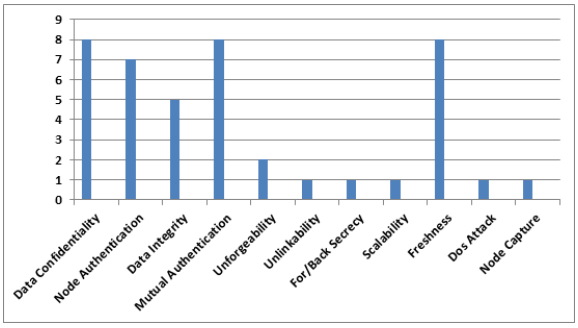

Fig 7. Analysis of Physiological Key Agreement Schemes

Maximum algorithms have considered the parameters like data confidentiality, node authentication, data integrity, mutual authentication and freshness. The parameter unforgeability is less stressed upon. Unlinkability, forward/backward secrecy,

Table 3. Analysis of Traditional Key Agreement Schemes

Scheme Used	Data Confidentiality	Node Authentication	Data Integrity	Mutual Authentication	Unforgeability	Unlinkability	Forward/ Backward Secrecy	Scalability	Freshness (key update)	Dos Attack	Node Capture Attack
(41)	Yes			Yes	Yes				Yes		
(43)				Yes				Yes			
(44)				Yes				Yes			
(45)							F/B				
(46)											
(47)	Yes	Yes		Yes				Yes	Yes		
(48)	Yes		Yes	Yes			F		Yes		
(49)				Yes	Yes						
(50)				Yes			F				
(51)		Yes					F/B				Yes
(55)							F				
(56)	Yes		Yes						Yes		
(57)		Yes		Yes					Yes		Yes
(58)	Yes	Yes		Yes			F				
(39)	Yes	Yes	Yes	Yes							
(59)	Yes	Yes					F/B		Yes		
(60)	Yes										Yes
(62)				Yes			F				
(63)				Yes		Yes	F/B				Yes
(64)	Yes										
(65)	Yes	Yes		Yes		Yes	F/B			Yes	
(66)				Yes			F/B		Yes	Yes	Yes
(68)				Yes							
(69)							F/B	Yes	Yes		Yes
(71)	Yes	Yes		Yes						Yes	
(72)							F/B		Yes		Yes
(73)		Yes		Yes			F				
(74)				Yes		Yes	F/B		Yes		Yes
(75)		Yes	Yes	Yes			F/B	Yes			
(76)	Yes	Yes		Yes	Yes				Yes		
30	12	10	4	19	3	3	15/10	5	11	3	8

Table 4. Analysis of Physiological Key Agreement Schemes

Scheme Used	Data Confidentiality	Node Authentication	Data Integrity	Mutual Authentication	Unforgeability	Unlinkability	Forward/ Backward Secrecy	Scalability	Freshness	Dos Attack	Node Capture Attack
(85)	Yes		Yes								
(86)	Yes	Yes	Yes	Yes					Yes		
(89)				Yes					Yes		
(90)	Yes	Yes	Yes	Yes	Yes	Yes			Yes		Yes
(91)	Yes	Yes	Yes	Yes					Yes		
(92)	Yes	Yes	Yes	Yes					Yes		
(79)	Yes	Yes		Yes	Yes		F	Yes	Yes	Yes	
(93)	Yes	Yes		Yes					Yes		
(95)	Yes	Yes		Yes					Yes		
9	8	7	5	8	2	1	1/0	1	8	1	1

scalability, DoS attack and Node capture attack are rarely bothered by the proposed schemes.

8.3 Analysis of Signal Based Key Agreement Schemes

Table 5 is prepared to show a comparison of different Signal based key agreement schemes.

Table 5. Analysis of Signal based Key Agreement Schemes

Scheme Used	Data Confidentiality	Node Authentication	Data Integrity	Mutual Authentication	Unforgeability	Unlinkability	Forward/ Backward Secrecy	Scalability	Freshness	Dos Attack	Node Capture Attack
(101)	Yes								Yes		
(103)	Yes								Yes		
(104)	Yes	Yes		Yes	Yes						Yes
(13)	Yes	Yes		Yes	Yes				Yes		Yes
(105)	Yes	Yes		Yes							
(106)	Yes	Yes		Yes					Yes		
(107)	Yes	Yes		Yes					Yes		
(108)	Yes	Yes		Yes							
(109)	Yes	Yes		Yes							
(110)									Yes		
(115)		Yes		Yes							Yes
11	9	8	0	8	2	0	0	0	6	0	3

Eleven algorithms are studied in Signal based key agreement scheme. A summary of the study is shown in Figure 8.

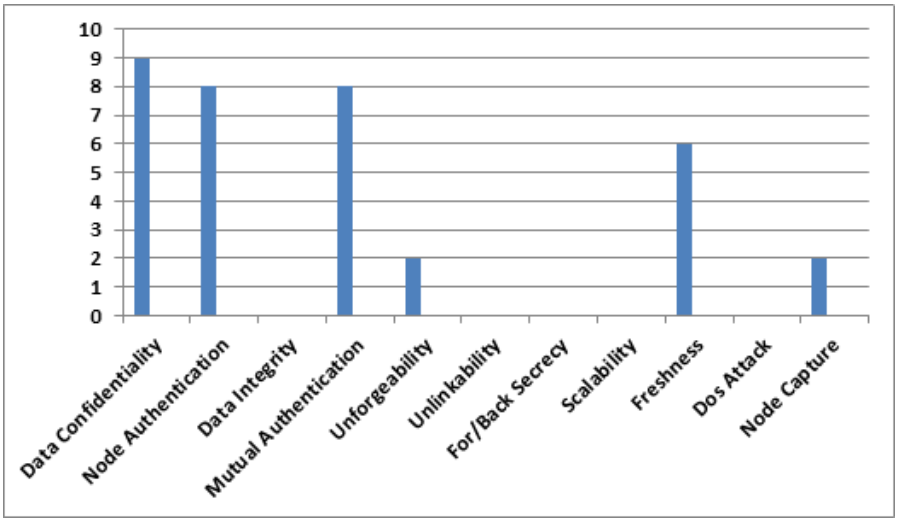

Fig 8. Analysis of Signal based Key Agreement Schemes

Maximum algorithms have considered the parameters like data confidentiality, node authentication, mutual authentication and freshness. The parameters like unforgeability and node capture attack are less stressed upon. None of the algorithm has considered data integrity, unlinkability, forward/backward secrecy, scalability and DoS attack.

8.4 Analysis of Hybrid Key Agreement Schemes

Table 6 is prepared to show a comparison of different Hybrid key agreement schemes.

Nine algorithms are studied in Hybrid key agreement scheme. A summary of the study is shown in Figure 9.

Maximum algorithms have considered the parameters like data confidentiality, node authentication, data integrity, mutual authentication and freshness. The parameters like unlinkability, forward/backward secrecy, DoS attack and node capture attack

Table 6. Analysis of Hybrid Key Agreement Schemes

Scheme Used	Data Confi-dentiality	Node Authenti-cation	Data Integrity	Mutual Authenti-cation	Unforge-ability	Unlink-ability	Forward/ Backward Secrecy	Scal-abil-ity	Fresh-ness	Dos Attack	Node Capture Attack
(119)	Yes		Yes			Yes			Yes		
(120)	Yes	Yes		Yes					Yes		
(121)	Yes	Yes		Yes			F		Yes	Yes	Yes
(122)	Yes	Yes		Yes					Yes		
(123)	Yes	Yes	Yes						Yes		
(124)	Yes			Yes					Yes		
(126)	Yes	Yes	Yes	Yes							
(126)	Yes								Yes		
(127)	Yes	Yes	Yes	Yes			F/B		Yes	Yes	Yes
9	9	6	4	6	0	1	2/1	0	8	2	2

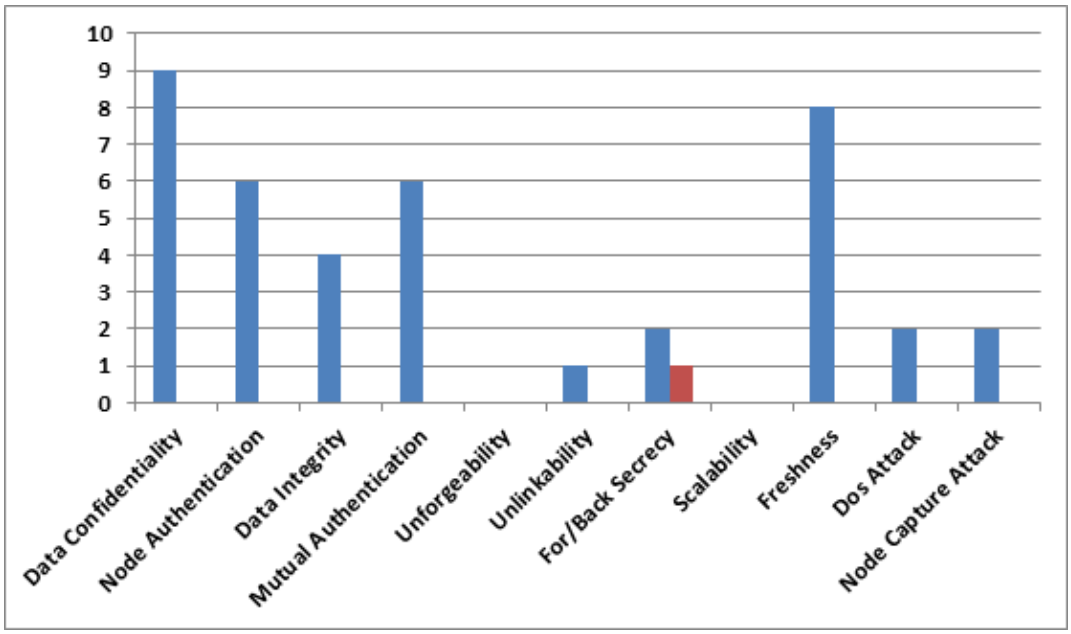

Fig 9. Analysis of Hybrid Key Agreement Schemes

are less stressed upon. None of the algorithm has discussed about unforgeability, and scalability.

Table 7 depicts the comparison of different schemesof all the four categories on the basis of additional parameters of security viz. hash function, Symmetric/ Asymmetric cryptography used, memory efficiency, computational efficiency, and energy efficiency.

Table 7. Comparison of key agreement schemes on the basis of additional parameters

Scheme Used	Hash	Symmetric Key	Asymmetric Key	Consider Memory Efficiency	Consider Computational Efficiency	Consider Energy Efficiency
(41)	HASH	Yes				
(43)		Yes			Yes	
(44)	MAC	Yes		Yes		Yes
(45)	MAC	Yes		Yes	Yes	Yes
(47)		Yes				Yes
(48)		Yes		Yes	Yes	Yes

Continued on next page

Table 7 continued

(50)	HASH	Yes				
(51)	HASH	Yes		Yes		Yes
(55)	MAC		Yes	Yes		
(57)			Yes			Yes
(39)	HASH					
(59)	MAC		Yes		Yes	
(60)			Yes	Yes	Yes	
(62)	HASH	Yes			Yes	
(63)	HASH			Yes	Yes	Yes
(64)	SHA-1		Yes	Yes	Yes	
(65)	HASH		Yes	Yes	Yes	
(66)	HASH	Yes	Yes	Yes	Yes	Yes
(68)		Yes	Yes		Yes	
(69)	HASH	Yes		Yes	Yes	Yes
(71)	HASH		Yes	Yes	Yes	Yes
(72)	HASH	Yes		Yes	Yes	Yes
(73)	HASH	Yes	Yes			
(74)	HASH		Yes	Yes	Yes	Yes
(75)	HASH				Yes	Yes
(76)	HASH	Yes				
(85)	MAC	Yes		Yes	Yes	
(86)	HASH	Yes		Yes	Yes	Yes
(89)		Yes			Yes	
(90)	MAC	Yes				
(91)	HASH	Yes		Yes	Yes	Yes
(92)	MD5	Yes	Yes		Yes	
(79)	MAC	Yes				Yes
(93)	MAC	Yes				
(95)	MAC	Yes				
(101)		Yes				
(103)		Yes		Yes	Yes	Yes
(104)		Yes				
(104)		Yes				
(103)		Yes				
(104)		Yes				
(13)		Yes				
(105)		Yes				
(106)		Yes				
(107)	MAC					
(112)		Yes		Yes	Yes	Yes
(116)	HASH	Yes				
(117)		Yes				
(118)		Yes		Yes		Yes
(119)	MAC	Yes				
(121)		Yes	Yes			
(122)	MAC	Yes	Yes		Yes	Yes
(123)	Digital Signature /Hash	Yes	Yes			
(124)	HASH	Yes		Yes		Yes
54	34	42	15		24	21

Summary of the study is shown in Figure 10

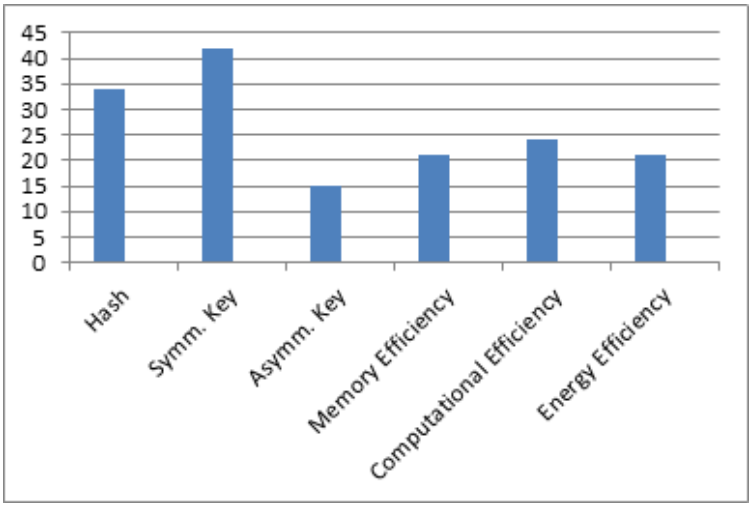

Fig 10. Comparison of the algorithms on additional parameters

Fifty four algorithms of all the different key agreement schemes are reviewed on the considered parameters. Around 60 percent algorithms have used hash methods either in their internal mechanism or to maintain the data integrity. Most of the algorithms are based on Symmetric key cryptography as it is lightweight in comparison of asymmetric key cryptography. In few cases, Symmetric as well as Asymmetric key cryptography have been used simultaneously for encryption process. Around one-third of the total algorithms have considered either memory or computation or energy efficiency in their designing.

The overall analysis highlights that there is scope of significant improvement is still available in the discussed schemes. The other research works also highlights similar trends but a one to one analysis of the reviewed schemes covered in this work with their work could not be possible. The lists of the reviewed schemes are found to be dissimilar due to the difference in the methodology and search criteria.

9 Conclusion

In this review work, a brief introduction of WBAN architecture in compliance with IEEE 80.15.6 is discussed first. Some of the differences between WSN and WBAN are also discussed. A total of eleven parameters are identified primarily during literature survey viz. data confidentiality, node authentication, data integrity, mutual authentication, unforgeability, unlinkability, forward/backward secrecy, scalability, freshness, dos attack and node capture attack. Taxonomy is provided to analyze different key agreement schemes based upon the identified security parameters. Performance analysis of the covered schemes is also conducted on the basis of usage of symmetric/asymmetric key, memory efficiency, computation efficiency and energy efficiency.

During analysis, it is observed that the prevention of DoS attack is not considered prominently in any of key agreement scheme. None of Signal based algorithm considered DoS attack whereas only one algorithm considered DoS attack in Physiological, two in Hybrid and three in Traditional key agreement scheme. Wireless environment is always susceptible to DoS attack. It should be taken into consideration while designing key agreement algorithms. Absence of DoS attack protection may trigger a crash. Few algorithms of Traditional key agreement scheme have considered Forward Secrecy and Backward Secrecy in their designing but it is rarely considered in other key agreement schemes. A few algorithms have considered Scalability in Traditional and Physiological scheme but none of the Signal based and Hybrid scheme algorithm considered this parameter. System must ensure security keeping in view of the inclusion of more nodes without causing any security flaw. Forward/ Backward secrecy and Scalability should be taken into consideration while designing key agreement algorithms. Data Integrity is considered moderately by all the schemes except Signal Based algorithms. Avoiding the data integrity could be dangerous in life critical situations. System must detect any modification in data during transit. Unlinkability is hardly bothered by any of the scheme. Like Unlinkability, Unforgeability is also overlooked by the algorithms. A compromised server may divert all the medical data towards the attacker which can play disastrous to the system. Data integrity, Unlinkability and Unfogeability should be taken into consideration while designing key agreement algorithms.

The main difference between WBAN and other networks is due to the size of hardware. Each node in WBAN has a limited energy with limited computational power and very small size of memory. All the operations must be designed to work keeping

in view of these limitations. In order to implement the key agreement schemes, additional lines of code would be required. It may impact the efficiency of the overall WBAN functioning. Very few algorithms have considered all the factors of efficiency. Even some algorithms have considered none of them.

This review emphasizes the importance of the security countermeasures while designing the key agreement schemes for WBAN environment. It also highlights the role of performance parameters during the development of such schemes. This work will benefit the future investigators, researchers and professionals to develop security preserving key agreement schemes for WBAN. WBAN implementation will improve the quality of life and also cut down the cost of expenditure incurred on health but the security flaws can play disaster for patients' health and prevent WBAN from being adopted.

References

1) Islam SMR, Kwak D, Kabir MH, Hossain M, Kyung A, Kwak S. The Internet of Things for Health Care: A Comprehensive Survey. *IEEE Access*. 2015.
2) Shokeen S, Parkash D. A Systematic Review of Wireless Body Area Network. In: IEEE 2019 International Conference on Automation, Computational and Technology Management (ICACTM). 2019;p. 58–62.
3) IoT analytics. . Available from: https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b.
4) Patient Monitoring Market- Segmented by Type of Device. *Trends, and Forecast*. 2018.
5) Kouicem DE, Bouabdallah A, Lakhlef H. Internet of things security: A top-down survey. *Computer Networks*. 2018;141:199–221. Available from: https://dx.doi.org/10.1016/j.comnet.2018.03.012.
6) Hajar MS, Al-Kadri MO, Kalutarage HK. A survey on wireless body area networks: architecture, security challenges and research opportunities. *Computers & Security*. 2021;104. Available from: https://dx.doi.org/10.1016/j.cose.2021.102211.
7) Hussain SZ, Kumar M. Secret Key Agreement Schemes in IOT Based Wireless Body Area Network. In: IEEE 2019 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT). 2019;p. 1–5.
8) Latré B, Braem B, Moerman I, Blondia C, Demeester P. A survey on wireless body area networks. *Wireless Networks*. 2011;17:1–18. Available from: https://dx.doi.org/10.1007/s11276-010-0252-4.
9) Nabi M, Geilen M, Basten T. On-demand data forwarding for automatic adaptation of data propagation in WBANs. In: 2012 9th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON). 2012;p. 326–334.
10) Tavera CA, Ortiz JH, Khalaf OI, Saavedra DF, Aldhyani THH. Wearable Wireless Body Area Networks for Medical Applications. *Computational and Mathematical Methods in Medicine*. 2021;2021:1–9. Available from: https://dx.doi.org/10.1155/2021/5574376.
11) Lee I, Lee K. The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons*. 2015;58(4):431–440. Available from: https://dx.doi.org/10.1016/j.bushor.2015.03.008.
12) Masdari M, Ahmadzadeh S, Bidaki M. Key management in wireless Body Area Network: Challenges and issues. *Journal of Network and Computer Applications*. 2017;91:36–51. Available from: https://dx.doi.org/10.1016/j.jnca.2017.04.008.
13) Shi L, Yuan J, Yu S, Li M. MASK-BAN: Movement-Aided Authenticated Secret Key Extraction Utilizing Channel Characteristics in Body Area Networks. *IEEE Internet of Things Journal*. 2015;2(1):52–62. Available from: https://dx.doi.org/10.1109/jiot.2015.2391113.
14) Jing Q, Vasilakos AV, Wan J, Lu J, Qiu D. Security of the Internet of Things: perspectives and challenges. *Wireless Networks*. 2014;20:2481–2501. Available from: https://dx.doi.org/10.1007/s11276-014-0761-7.
15) Mainanwal V, Gupta M, Upadhayay SK. A survey on wireless body area network: Security technology and its design methodology issue. *IEEE 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*. 2015;p. 1–5.
16) Al-Janabi S, Al-Shourbaji I, Shojafar M, Shamshirband S. Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. *Egyptian Informatics Journal*. 2017;18(2):113–122. Available from: https://dx.doi.org/10.1016/j.eij.2016.11.001.
17) Usman M, Asghar MR, Ansari IS, Qaraqe M. Security in Wireless Body Area Networks: From In-Body to Off-Body Communications. *IEEE Access*. 2018;6:58064–58074. Available from: https://dx.doi.org/10.1109/access.2018.2873825.
18) Bharathi RS, Venkateswari KR. Security Challenges and Solutions for Wireless Body Area Networks. In: B I, S N, N P, editors. Computing, Communication and Signal Processing;vol. 810. Springer. 2019. Available from: https://doi.org/10.1007/978-981-13-1513-8_29.
19) Kompara M, Hölbl M. Survey on security in intra-body area network communication. *Ad Hoc Networks*. 2018;70:23–43. Available from: https://dx.doi.org/10.1016/j.adhoc.2017.11.006.
20) Chaudhary S, Singh A, Chatterjee K. Wireless Body Sensor Network (WBSN) Security and Privacy Issues: A Survey. *International Journal of Computational Intelligence & IoT*. 2019;2(2). Available from: https://ssrn.com/abstract=3355560.
21) Hasan K, Biswas K, Ahmed K, Nafi NS, Islam MS. A comprehensive review of wireless body area network. *Journal of Network and Computer Applications*. 2019;143:178–198. Available from: https://dx.doi.org/10.1016/j.jnca.2019.06.016.
22) Jabeen T, Ashraf H, Ullah A. A survey on healthcare data security in wireless body area networks. *Journal of Ambient Intelligence and Humanized Computing*. 2021. Available from: https://dx.doi.org/10.1007/s12652-020-02728-y.
23) Liu Q, Mkongwa KG, Zhang C. Performance issues in wireless body area networks for the healthcare application: a survey and future prospects. *SN Applied Sciences*. 2021;3(2):155–155. Available from: https://dx.doi.org/10.1007/s42452-020-04058-2.
24) Kumari R, Nand P. Performance comparison of various routing protocols in WSN and WBAN. *2016 International Conference on Computing, Communication and Automation (ICCCA)*. 2016;p. 427–431. Available from: 10.1109/CCAA.2016.7813814.
25) Kwak KS, Ullah S, Ullah N. An overview of IEEE 802.15.6 standard. In: IEEE 3rd International Symposium on Applied Sciences in Biomedical and Communication Technologies. 2010;p. 1–6. doi:10.1109/ISABEL.2010.5702867.
26) Toorani M. On Vulnerabilities of the Security Association in the IEEE 802.15.6 Standard. *Springer International Conference on Financial Cryptography and Data Security*. 2015. Available from: https://doi.org/10.1007/978-3-662-48051-9_18.
27) Huang C, Lee H, Lee DH. A Privacy-Strengthened Scheme for E-Healthcare Monitoring. *Journal of Medical Systems (Springer)*. 2012;36(5):2959–2971. Available from: https://doi.org/10.1007/s10916-011-9774-2.
28) Ameen M, Liu J, Kwak K. Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications. *Journal of Medical Systems(Springer)*. 2012;36(1):93–101. Available from: https://doi.org/10.1007/s10916-010-9449-4.

29) Ali A, Khan FA. Key Agreement Schemes in Wireless Body Area Networks: Taxonomy and State-of-the-Art. *Journal of Medical Systems*. 2015;39(115). Available from: https://doi.org/10.1007/s10916-015-0272-9.
30) Ma L, Ge Y, Zhu Y. TinyZKP: A lightweight authentication scheme based on zero knowledge proof for wireless body area networks. *Wireless Personal Communications (Springer)*. 2014;77(2):1077–1090. Available from: 10.1007/s11277-013-1555-4.
31) Yao L, Liu B, Yao K, Wu G, Wang J. An ECG-Based Signal Key Establishment Protocol in Body Area Networks. In: IEEE 7th International Conference on Autonomic & Trusted Computing. 2010;p. 233–238.
32) Bao S, Carmen CYP, Shen L, Zhang Y. Authenticated symmetric-key establishment for medical body sensor networks. *Journal of Electronics (China)*. 2007;24(3):421–427. Available from: https://dx.doi.org/10.1007/s11767-006-0152-z.
33) Drira W, Renault E, Zeghlache D. A Hybrid Authentication and Key Establishment Scheme for WBAN. In: 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications. 2012;p. 78–83.
34) Tan CC, Wang H, Zhong S, Li Q. IBE-Lite: A Lightweight Identity-Based Cryptography for Body Sensor Networks. *IEEE Transactions on Information Technology in Biomedicine*. 2009;13:926–932.
35) García-Morchón O, Gómez-Pérez D, Gutiérrez J, Rietman R, Schoenmakers B, Tolhuizen L. HIMMO: A Lightweight Collusion-Resistant Key Predistribution Scheme. *Cryptology ePrint Archive: Report 2014/698*. Available from: https://eprint.iacr.org/2014/698.
36) Chalkias K, Mpaldimtsi F, Hristu-Varsakelis D, Stephanides G. On The Key Compromise Impersonation Vulnerability Of One-Pass Key Establishment Protocols. *International Conference on Security and Cryptography (SECRYPT)*. 2007;p. 222–228.
37) Cherukuri S, Venkatasubramanian KK, Gupta SKS. Biosec: a biometric based approach for securing communication in wireless networks of biosensors implanted in the human body. In: IEEE International Conference on Parallel Processing Workshops Proceedings. 2003;p. 432–439.
38) Liu J, Li Q, Yan R, Sun R. Efficient authenticated key exchange protocols for wireless body area networks. *EURASIP Journal on Wireless Communications and Networking*. 2015;2015(1):188–188. Available from: https://doi.org/10.1186/s13638-015-0406-2.
39) Lee YS, Alasaarela E, Lee H. Secure key management scheme based on ECC algorithm for patient's medical information in healthcare system. In: IEEE International Conference on Information Networking 2014 (ICOIN2014). 2014;p. 453–457. Available from: 10.1109/ICOIN.2014.6799723.
40) Amin NU, Asad M, Nizamuddin SA, Chaudhry. An authenticated key agreement with rekeying for secured body sensor networks based on hybrid cryptosystem. In: Proceedings of 2012 9th IEEE International Conference on Networking, Sensing and Control. ;p. 118–121. Available from: 10.1109/ICNSC.2012.6204902.
41) Kumar P, Lee SG, Lee HJ. E-SAP: Efficient-strong authentication protocol for healthcare applications using wireless medical sensor networks. *Sensors*;12(2). Available from: https://doi.org/10.3390/s120201625.
42) Masdari M, Ahmadzadeh S, Bidaki M. Key management in wireless Body Area Network: Challenges and issues. *Journal of Network and Computer Applications*. 2017;91:36–51. Available from: https://dx.doi.org/10.1016/j.jnca.2017.04.008.
43) Sanchez DS, Baldus H. A Deterministic Pairwise Key Pre-distribution Scheme for Mobile Sensor Networks. In: IEEE First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05). 2005;p. 277–288. doi:10.1109/SECURECOMM.2005.2.
44) Morchon OG, Baldus H, Sanchez DS. Resource-efficient security for medical body sensor networks. In: IEEE International Workshop on Wearable and Implantable Body Sensor Networks (BSN'06). 2006;p. 4–83. doi:10.1109/BSN.2006.45.
45) Ren Y, Oleshchuk V, Li FY, Sulistyo S. FoSBaS: A bi-directional secrecy and collusion resilience key management scheme for BANs. In: IEEE Wireless Communications and Networking Conference (WCNC). 2012;p. 2841–2846. Available from: 10.1109/WCNC.2012.6214286.
46) Morchon OG, Baldus H. Efficient distributed security for wireless medical sensor networks. In: IEEE International Conference on Intelligent Sensors, Sensor Networks and Information Processing. 2008;p. 249–254. doi:10.1109/ISSNIP.2008.4761995.
47) Lamichhane B, Mudda S, Regazzoni F, Puiatti A. LEXCOMM: A low energy, secure and flexible communication protocol for a heterogenous body sensor network. In: IEEE-EMBS International Conference on Biomedical and Health Informatics. 2012;p. 273–276. doi:10.1109/BHI.2012.6211564.
48) Selimis G, Huang L, Massé F, Tsekoura I, Ashouei M, Catthoor F, et al. A Lightweight Security Scheme for Wireless Body Area Networks: Design, Energy Evaluation and Proposed Microprocessor Design. *Journal of Medical Systems*. 2011;35(5):1289–1298. Available from: https://dx.doi.org/10.1007/s10916-011-9669-2.
49) He D, Kumar N, Chen J, Lee CC, Chilamkurti N, Yeo SS. Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks. *Multimedia Systems*. 2015;21(1):49–60. Available from: https://dx.doi.org/10.1007/s00530-013-0346-9.
50) Li M, Yu S, Lou W, Ren K. Group Device Pairing based Secure Sensor Association and Key Management for Body Area Networks. *IEEE INFOCOM*. 2010;p. 1–9. Available from: 10.1109/INFCOM.2010.5462095.
51) Li M, Yu S, Guttman JD, Lou W, Ren K. Secure ad hoc trust initialization and key management in wireless body area networks. *ACM Transactions on Sensor Networks*. 2013;9(2):1–35. Available from: https://dx.doi.org/10.1145/2422966.2422975.
52) Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*. 1978;21(2):120–126. Available from: https://dx.doi.org/10.1145/359340.359342.
53) Li M, Lou W, Ren K. Data security and privacy in wireless body area networks. *IEEE Wireless Communications*. 2010;17(1):51–58. Available from: 10.1109/MWC.2010.5416350.
54) Gura N, Patel A, Wander A, Eberle H, Shantz SC. Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs. In: M J, JJ Q, editors. Cryptographic Hardware and Embedded Systems - CHES;vol. 3156. Springer. 2004. doi:https://doi.org/10.1007/978-3-540-28632-5_9.
55) Malan DJ, Welsh M, Smith MD. A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography. In: First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks. 2004;p. 71–80. doi:10.1109/SAHCN.2004.1381904.
56) Liu J, Kwak KS. Hybrid security mechanisms for wireless body area networks. In: IEEE Second International Conference on Ubiquitous and Future Networks (ICUFN). 2010;p. 98–103. doi:10.1109/ICUFN.2010.5547221.
57) Huang X, Wang Q, Bangdao C, Markham A, Jäntti R, Roscoe AW. Body sensor network key distribution using human interactive channels. *ACM 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies*. 2011. Available from: https://doi.org/10.1145/2093698.2093841.
58) Ho J. A versatile suite of strong authenticated key agreement protocols for body area networks. In: IEEE 8th International Wireless Communications and Mobile Computing Conference (IWCMC). 2012;p. 683–688. doi:10.1109/IWCMC.2012.6314287.
59) Shen J, Tan H, Moh S, Chung I, Liu Q, Sun X. Enhanced secure sensor association and key management in wireless body area networks. *Journal of Communications and Networks*. 2015;17(5):453–462. Available from: https://dx.doi.org/10.1109/jcn.2015.000083.
60) Tan CC, Wang H, Zhong S, Li Q. Body Sensor network security: an identity based cryptography approach. 2008;p. 148–153. Available from: https://doi.org/10.1145/1352533.1352557.

61) Li X, Ibrahim MH, Kumari S, Sangaiah AK, Gupta V, Choo KKR. Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks. *Computer Networks*. 2017;129:429–443. Available from: https://dx.doi.org/10.1016/j.comnet.2017.03.013.
62) Chen CM, Xiang B, Wu TY, Wang KH. An Anonymous Mutual Authenticated Key Agreement Scheme for Wearable Sensors in Wireless Body Area Networks" in Applied. *Sciences*. 2018;8(7):1074. Available from: https://doi.org/10.3390/app8071074.
63) Narwal B, Mohapatra AK. SEEMAKA: Secured Energy-Efficient Mutual Authentication and Key Agreement Scheme for Wireless Body Area Networks" in Wireless Personal Communications. *Wireless Personal Communications*. 1985;113:1985–2008. Available from: https://doi.org/10.1007/s11277-020-07304-3.
64) Ali M, Sadeghi MR, Liu X. Lightweight Fine-Grained Access Control for Wireless Body Area Networks. *Sensors*. 2020;20(4). Available from: https://doi.org/10.3390/s20041088.
65) Singh U, Narwal B. A Novel Authentication Scheme for Wireless Body Area Networks with Anonymity. In: R PC, B P, P M, R B, KC L, editors. Progress in Advanced Computing and Intelligent Engineering. Advances in Intelligent Systems and Computing;vol. 1198. Springer. 2021.
66) Mo J, Shen W, Pan W. An Improved Anonymous Authentication Protocol for Wearable Health Monitoring Systems. *Wireless Communications and Mobile Computing*. 2020;2020:1–13. Available from: https://dx.doi.org/10.1155/2020/5686498.
67) Jiang Q, Ma J, Yang C, Ma X, Shen J, Chaudhry SA. Efficient end-to-end authentication protocol for wearable health monitoring systems. *Computers & Electrical Engineering*. 2017;63:182–195. Available from: https://dx.doi.org/10.1016/j.compeleceng.2017.03.016.
68) Murthy GSN, Rao SV, Pullela MSK, Ram K. A Hybrid Advanced Encryption Scheme for a Protected Wireless Sensor data in Secure transmission and Storage. *International Journal of Advanced Science and Technology*. 2020;29(11s):506–515. Available from: http://sersc.org/journals/index.php/IJAST/article/view/20010.
69) Rehman ZU, Altaf S, Iqbal S. An Efficient Lightweight Key Agreement and Authentication Scheme for WBAN. *IEEE Access*. 2020;8:175385–175397. Available from: https://dx.doi.org/10.1109/access.2020.3026630.
70) Kompara M, Islam SH, Hölbl M. A robust and efficient mutual authentication and key agreement scheme with untraceability for WBANs. *Computer Networks*. 2019;148:196–213. Available from: https://dx.doi.org/10.1016/j.comnet.2018.11.016.
71) Gautam AK, Kumar R. Secure new node ID assignment for internet integrated wireless body area networks. *EAI Endorsed Transactions on Scalable Information Systems*. 2020;7(28):107–114. Available from: 10.4108/eai.13-7-2018.164554.
72) Meng X, Xu J, Wu X, Wang Z. Design of a mutual authentication and key agreement protocol for WBANs. *Journal of Information Hiding and Privacy Protection*. 2020;2(3):107–114. Available from: 10.32604/jihpp.2020.09901.
73) Shen J, Moh S, Chung I. A Novel Key Management Protocol in Body Area Networks. *The 7th International Conference on Networking and Services*. 2011;p. 246–251.
74) Ibrahim MH, Kumari S, Das AK, Wazid M, Odelu V. Secure anonymous mutual authentication for star two-tier wireless body area networks. *Computer Methods and Programs in Biomedicine*. 2016;135:37–50. Available from: https://dx.doi.org/10.1016/j.cmpb.2016.07.022.
75) Almuhaideb AM, Alqudaihi KS. A Lightweight and Secure Anonymity Preserving Protocol for WBAN. *IEEE Access*. 2020;8:178183–178194. Available from: https://dx.doi.org/10.1109/access.2020.3025733.
76) Song Y, Tan H. Practical pairing-Free sensor cooperation scheme for cloud-Assisted wireless body area networks. *Cybersecurity*. 2020;3(1):21. Available from: https://dx.doi.org/10.1186/s42400-020-00061-7.
77) Zhao H, Xu R, Shu M, Hu J. Physiological-signal-based key negotiation protocols for body sensor networks: A survey. *Simulation Modelling Practice and Theory*. 2016;0:1–13. Available from: https://doi.org/10.1016/j.simpat.2015.12.003.
78) Venkatasubramanian KK, Banerjee A, Gupta SKS. PSKA: Usable and Secure Key Agreement Scheme for Body Area Networks. *IEEE Transactions on Information Technology in Biomedicine*. 2010;14:60–68. Available from: 10.1109/TITB.2009.2037617.
79) Ali A, Khan FA. A Broadcast-Based Key Agreement Scheme Using Set Reconciliation for Wireless Body Area Networks". *Journal of Medical Systems*. 2014;38(5):33. Available from: https://doi.org/10.1007/s10916-014-0033-1.
80) Ali A, Irum S, Kausar F, Khan FA. A cluster-based key agreement scheme using keyed hashing for Body Area Networks. *Multimedia Tools and Applications*. 2013;66:201–214. Available from: https://doi.org/10.1007/s11042-011-0791-4.
81) Miao F, Bao SD, Li Y. Biometric key distribution solution with energy distribution information of physiological signals for body sensor network security. *IET Information Security*. 2013;7(2):87–96. Available from: https://dx.doi.org/10.1049/iet-ifs.2012.0104.
82) Venkatasubramanian KK, Banerjee A, Gupta SKS. Plethysmogram-based secure inter-sensor communication in Body Area Networks. In: MILCOM 2008 IEEE Military Communications Conference. ;p. 1–7. doi:10.1109/MILCOM.2008.4753199.
83) Kanjee MR, Divi K, Liu H. A Physiological Authentication Scheme in Secure Healthcare Sensor Networks. In: 7th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON). 2010;p. 1–3. doi:10.1109/SECON.2010.5508215.
84) Poon CCY, Zhang YT, Bao SD. A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. *IEEE Communications Magazine*. 2006;44(4):73–81. Available from: https://dx.doi.org/10.1109/mcom.2006.1632652.
85) Hu C, Cheng X, Zhang F, Wu D, Liao X, Chen D. OPFKA: Secure and efficient Ordered-Physiological-Feature-based key agreement for wireless Body Area Networks. *Proceedings IEEE INFOCOM*. 2013;p. 2274–2282. Available from: 10.1109/INFCOM.2013.6567031.
86) Jammali N, Fourati LC. PFKA: A physiological feature based key agreement for wireless body area network. In: IEEE International Conference on Wireless Networks and Mobile Communications (WINCOM). 2015;p. 1–8. doi:10.1109/WINCOM.2015.7381316.
87) Cao C, He C, Bao S, Li Y. Improvement of fuzzy vault scheme for securing key distribution in body sensor network. In: Annual International Conference of the IEEE Engineering in Medicine and Biology Society. 2011;p. 3563–3567. doi:10.1109/IEMBS.2011.6090594.
88) Rajasekaran RT, Manjula V, Kishore V, Sridhar TM, Jayakumar C. An Efficient and Secure Key Agreement Scheme Using Physiological Signals in Body Area Networks. *ACM International Conference on Advances in Computing, Communications and Informatics*. 2012. Available from: https://doi.org/10.1145/2345396.2345579.
89) Zaghouani EK, Jemai A, Benzina A, Attia R. ELPA: A new key agreement scheme based on linear prediction of ECG features for WBAN. In: IEEE 23rd European Signal Processing Conference (EUSIPCO). 2015;p. 81–85. doi:10.1109/EUSIPCO.2015.7362349.
90) Mana M, Feham M, Bensaber BA. Trust Key Management Scheme for Wireless Body Area Networks". *International Journal of Network Security*. 2011;12(2):71–79. Available from: 10.6633/IJNS.201103.12(2).02.
91) Yasmeen AS, Eman E, Ahmed A, Mohammed E. Ouda Osama "Efficient Key Agreement Algorithm for Wireless Body Area Networks Using Reusable ECG-Based Features. *Electronics*. 2021;10:404–404. Available from: 10.3390/electronics10040404.
92) Al-janabi STF, Dawood AJ, Hassan EH. Biometric-Based Authentication and Key Management Scheme for WBANs. *i-manager's Journal on Information Technology*. 2013;2(2):23–31. Available from: https://dx.doi.org/10.26634/jit.2.2.2286.

93) Venkatasubramanian KK, Banerjee A, Gupta SKS. EKG-based key agreement in Body Sensor Networks. *IEEE INFOCOM Workshops*. 2008;p. 1–6. Available from: 10.1109/INFOCOM.2008.4544608.
94) Ali A, Khan FA. An Improved EKG-Based Key Agreement Scheme for Body Area Networks. In: K BS, W A, T K, Y X, editors. Security and Assurance. ISA 2010;vol. 76. Springer. . doi:https://doi.org/10.1007/978-3-642-13365-7_29.
95) Juels A, Sudan M. A Fuzzy Vault Scheme. *Designs, Codes and Cryptography*. 2006;38(2):237–257. Available from: https://dx.doi.org/10.1007/s10623-005-6343-z.
96) Cho K, Lee D. Biometric based secure communications without pre-deployed key for biosensor implanted in body sensor networks. *Lecture Notes Computer Science*. 2012;7115:203–218. Available from: https://doi.org/10.1007/978-3-642-27890-7_17.
97) Shi J, Lam K, Gu M, Li M, Chung S. Towards Energy-Efficient Secure Communications Using Biometric Key Distribution in Wireless Biomedical Healthcare Networks. In: IEEE 2nd International Conference on Biomedical Engineering and Informatics. 2009;p. 1–5. doi:10.1109/BMEI.2009.5304940.
98) Venkatasubramanian KK, Gupta SKS. Physiological value-based efficient usable security solutions for body sensor networks. *ACM Transactions on Sensor Networks*. 2010;6(4):1–36. Available from: https://dx.doi.org/10.1145/1777406.1777410.
99) Revadigar G, Javali C, Asghar HJ, Rasmussen KB, Jha S. Mobility Independent Secret Key Generation for Wearable Health-care Devices. *ACM 10th EAI International Conference on Body Area Networks*. 2015;p. 294–300. Available from: https://doi.org/10.4108/eai.28-9-2015.2261446.
100) Ali ST, Sivaraman V, Ostry D. Zero reconciliation secret key generation for body-worn health monitoring devices. *Fifth ACM Conference Security and Privacy in Wireless and Mobile Networks*. 2012;p. 39–50. Available from: https://doi.org/10.1145/2185448.2185455.
101) Ali ST, Sivaraman V, Ostry D. Secret Key Generation Rate vs. Reconciliation Cost Using Wireless Channel Characteristics in Body Area Networks. In: IEEE/IFIP International Conference on Embedded and Ubiquitous Computing. 2010;p. 644–650. doi:10.1109/EUC.2010.103.
102) Yao L, Taha A, Sivaraman V, Ostry D. Improving Secret Key Generation Performance for On-Body Devices. In: BodyNets" 6th International Conference on Body Area Networks. 2011;p. 19–22. Available from: http://hdl.handle.net/102.100.100/102481?index=1.
103) Tsouri GR, Wilczewski J. Reliable symmetric key generation for body area networks using wireless physical layer security in the presence of an on-body eavesdropper. *Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies - ISABEL '11*. 2011;p. 1–6. Available from: https://doi.org/10.1145/2093698.2093851.
104) Shi L, Yuan J, Yu S, Li M. ASK-BAN: Authenticated Secret Key Extraction Utilizing Channel Characteristics for Body Area Networks. *Sixth ACM conference on Security and privacy in wireless and mobile networks*. 2013. Available from: https://doi.org/10.1145/2462096.2462123.
105) Javali C, Revadigar G, Libman L, Jha S. SeAK: Secure Authentication and Key Generation Protocol Based on Dual Antennas for Wireless Body Area Networks. In: Saxena N, Sadeghi AR, editors. Lecture Notes in Computer Science;vol. 8651. Springer. 2015. Available from: https://doi.org/10.1007/978-3-319-13066-8_5.
106) Li Z, Wang H, Daneshmand M, Fang H. Secure and efficient key generation and agreement methods for wireless body area networks. In: IEEE International Conference on Communications (ICC). 2017;p. 1–6. doi:10.1109/ICC.2017.7996848.
107) Li Z, Wang H. A key agreement method for wireless body area networks. In: IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). 2016;p. 690–695. doi:10.1109/INFCOMW.2016.7562165.
108) Pierson TJ, Liang X, Peterson R, Kotz D. Wanda: Securely introducing mobile devices. In: IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications. 2016;p. 1–9. doi:10.1109/INFOCOM.2016.7524366.
109) Wu Y, Sun Y, Zhan L, Ji Y. Low mismatch key agreement based on wavelet-transform trend and fuzzy vault in body area network. *International Journal of Distributed Sensor Networks*. 2013. Available from: https://doi.org/10.1155/2013/912873.
110) Bichler D, Stromberg G, Huemer M, Löw M. Key Generation Based on Acceleration Data of Shaking Processes. In: J K, D AG, A S, T S, editors. UbiComp 2007: Ubiquitous Computing. UbiComp;vol. 4717. Springer. 2007. doi:https://doi.org/10.1007/978-3-540-74853-3_18.
111) Mayrhofer R, Gellersen H. Shake Well Before Use: Intuitive and Secure Pairing of Mobile Devices. *IEEE Transactions on Mobile Computing*. 2009;8(6):792–806. Available from: https://dx.doi.org/10.1109/tmc.2009.51.
112) Quach Q, Nguyen N, Dinh T. Secure Authentication for Mobile Devices Based on Acoustic Background Fingerprint. In: V H, T D, D T, A L, S P, editors. Advances in Intelligent Systems and Computing;vol. 244. Springer. 2014. doi:https://doi.org/10.1007/978-3-319-02741-8_32.
113) Xu W, Revadigar G, Luo C, Bergmann N, Hu W. Walkie-Talkie: Motion-Assisted Automatic Key Generation for Secure On-Body Device Communication. In: 15th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN). 2016;p. 1–12. doi:10.1109/IPSN.2016.7460726.
114) Xu W, Javali C, Revadigar G, Luo C, Bergmann N, Hu W. Gait-Key: A Gait-Based Shared Secret Key Generation Protocol for Wearable Devices. *ACM Transactions on Sensor Networks*. 2017;13(1):1–27. Available from: https://doi.org/10.1145/3023954.
115) Umar M, Wu Z, Liao X. Channel Characteristics Aware Zero Knowledge Proof Based Authentication Scheme in Body Area Networks. *Ad Hoc Networks*. 102374;2021(112). Available from: https://doi.org/10.1016/j.adhoc.2020.102374.
116) Venkatasubramanian KK, Gupta SKS. Security for Pervasive Health Monitoring Sensor Applications. In: Fourth International Conference on Intelligent Sensing and Information Processing. 2006;p. 197–202. doi:10.1109/ICISIP.2006.4286096.
117) Bui FM, Hatzinakos D. 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*. 2007;2008(1). Available from: https://dx.doi.org/10.1155/2008/529879.
118) Zhao H, Qin J, Hu J. An Energy Efficient Key Management Scheme for Body Sensor Networks. *IEEE Transactions on Parallel and Distributed Systems*. 2013;24:2202–2210. Available from: 10.1109/TPDS.2012.320.
119) Jamali N, Fourati LC. SKEP: A secret key exchange protocol using physiological signals in wireless body area networks. In: IEEE International Conference on Wireless Networks and Mobile Communications (WINCOM). 2015;p. 1–7. doi:10.1109/WINCOM.2015.7381317.
120) Raazi SMK, Lee H, Lee S, Lee Y. BARI: A Distributed Key Management Approach for Wireless Body Area Networks. In: 2009 International Conference on Computational Intelligence and Security. 2009;p. 324–329. doi:10.1109/CIS.2009.186.
121) Muhammad KRRS, Lee H, Lee S, Lee YK. BARI+: a biometric based distributed key management approach for wireless body area networks. *Sensors*. 2010;10(4):3911–3944. Available from: 10.1109/CIS.2009.186.
122) Zhang GH, Poon CCY, Li Y, Zhang YT. A biometric method to secure telemedicine systems. In: Annual International Conference of the IEEE Engineering in Medicine and Biology Society. 2009;p. 701–704. doi:10.1109/IEMBS.2009.5332470.
123) Mana MM. SEKEBAN (Secure and Efficient Key Exchange for wireless Body Area Network. *International Journal of Advanced Science and Technology*. 2009;12:45–60. Available from: https://www.earticle.net/Article/A147319.
124) Xu F, Qin Z, Tan CC, Wang B, Li Q. IMDGuard: Securing implantable medical devices with the external wearable guardian. In: 2011 Proceedings IEEE INFOCOM. 2011;p. 1862–1870. doi:10.1109/INFCOM.2011.5934987.

125) Sankaran S, Husain MI, Sridhar R. IDKEYMAN: An Identity Based Key Management Scheme for Wireless Ad Hoc Body Area Networks. In: and others, editor. IDKEYMAN: An Identity Based Key Management Scheme for Wireless Ad Hoc Body Area Networks. . Available from: https://www.albany.edu/wwwres/conf/iasymposium/proceedings/2009/ASIA09FinalProceedings.pdf#page=32.
126) Sampangi RV, Dey S, Urs SR, Sampalli S. IAMKeys: Independent and Adaptive Management of Keys for Security in Wireless Body Area Networks. In: N M, N C, D N, editors. Advances in Computer Science and Information Technology. Computer Science and Information Technology. CCSIT 2012. Lecture Notes of the Institute for Computer Sciences;vol. 86. Springer. 2012. Available from: https://doi.org/10.1007/978-3-642-27317-9_49.
127) Sammoud A, Chalouf MA, Hamdi O, Montavont N, Bouallegue A. A new biometrics-based key establishment protocol in WBAN: energy efficiency and security robustness analysis. *Computers & Security*. 2020;96. Available from: https://dx.doi.org/10.1016/j.cose.2020.101838.
128) He D, Chen C, Chan S, Bu J, Zhang P. Secure and Lightweight Network Admission and Transmission Protocol for Body Sensor Networks. *IEEE Journal of Biomedical and Health Informatics*. 2013;17(3):664–674. Available from: https://dx.doi.org/10.1109/jbhi.2012.2235180.