Journal of Ambient Intelligence and Humanized Computing (2021) 12:9841–9854
https://doi.org/10.1007/s12652-020-02728-y

ORIGINAL RESEARCH

A survey on healthcare data security in wireless body area networks

Tallat Jabeen[1] · **Humaira Ashraf**[1] · **Ata Ullah**[2]

Received: 7 April 2020 / Accepted: 19 November 2020 / Published online: 2 January 2021

Abstract
Advances in remote interchanges, the internet of nano things have empowered the wireless body area networks (WBAN) to end up a promising systems of networking standard. It involves interconnected tiny sensors to gather ongoing biomedical data and transmit over the network for further analysis. Due to possibility of active and passive number of attacks, the healthcare data security is quite essential and challenging. This paper presents the systematic literature review (SLR) of the multiple security schemes for WBAN. We have identified a research question to analyses the possibility of several attacks while preserving the memory constraints. We have performed quality valuation to ensure the relevance of schemes with the research question. Moreover, the schemes are considered from 2016 to 2020 to focus on recent work. In literature, several existing schemes are explored to identify how the security is enhanced for exchanging patients' healthcare data. The data security schemes using AES, ECC, SHA-1 and hybrid encryption are analyzed based on influential traits. Several methodologies for data security in WBAN are considered and the most appropriate methodologies are appraised. We also analyses the security for different attack scenarios.

Keywords WBAN · Healthcare · Data security · Attack mitigation · SLR

1 Introduction

Wireless Body Area Networks (WBAN) comprises of the nano sensor nodes placed at the human body to gather and monitor patient's data. Body nodes collect data and transmit it towards the medical server through wireless channel (Al-Janabi 2016). Cryptographic procedures help in changing the original data into inconceivable information. There are two types of the WBAN's: intra WBAN and beyond WBAN. Intra WBAN includes nano sensors that are wearable and used by the human body while beyond WBAN refers a network where the gateway provides the connection link to the medical server. Sensor hubs are extremely restricted in computational limits, memory, and power. There are various measures of research to deal with information security in WBAN, and this analysis guarantee to work intensely in remote sensors on various viewpoints. It deals with WBAN environment and the supreme objective of the research is to secure patients' data from various attacks such as homing attack, Tempering attack, and plaintext Attack with less memory consumption.

Data security is quite essential for sharing the data over the public network where intruders can misuse or alter the data. Several attacks are possible to disturb the smooth transmission of data over wireless channel. In natural life observing or comparable situation, it might be uncritical to move unencrypted data and in plain content as typically any outsiders are not interested by such information, yet in numerous other situation, there is a necessity for secure and reliable data transmission. An example of natural life environment, health insurance may be interested about data of health condition and thieves may be interested in personal life activities. There are many scenarios that need security of data very intensely (Subbarayadu et al. 2016).

Existing literature provides details about data privacy and security but does not focus on the SLR and the criteria to collect material (Al-Janabi 2016). In Zou (2017), good

✉ Ata Ullah
aullah@numl.edu.pk

Tallat Jabeen
tallat_cs@yahoo.com

Humaira Ashraf
humaira.ashraf@iiu.edu.pk

[1] Department of Computer Science and Software Engineering, International Islamic University, Islamabad 44000, Pakistan

[2] Department of Computer Science, National University of Modern Languages (NUML), Islamabad, Pakistan

literature on security solutions but not concentrated on the security analysis for the literature. In Niksaz (2015), a number of attack scenarios and their solutions are explored but this may blurred the literature article linkages of inclusion and exclusion criteria. Another very important and good quality survey based on the SLR is rationalized (Paul 2019) but it used a smaller amount of existing literature which may affect the comparisons of techniques. Additionally, a systematic review (Shokeen 2019) is also focused to compare and underline the gapes of research, this survey does not give many particulars about existing schemes of WBAN literature. A systematic literature review is performed in the study (Kitchenham 2008; Okoli 2010; Wohlin 2014) which are followed to support the proposed SLR in survey. A staggering amount of $7 trillion is expended on various healthcare systems worldwide, out of which $585 billion is lost on missed opportunities. The introduction of modern and better technologies has greatly affected healthcare (Vora 2018).

Over the past few decades, data has become a primary source of knowledge and provides new possibilities for real-life issues.

These applications are data driven and integrate actionable insights into user experience which helps individuals to complete the desired task more effectively. It operationalizes insights, customizes customer experience, optimizes customer experiences, increases operating performance, and allows for new business model. A robust Intrusion Detection Program to tackle the above-mentioned problem (IDS) is required as conventional approaches use a signature-based approach to detect patterns. Yet one of the new technologies known as ML can be used to analyses the data traffic to detect intrusions and attack patterns. Therefore, reliable, and powerful algorithms for analyzing this vast amount of data are in dire need of managing smart applications based on blockchain (Tanwar 2019).

Security systems based on Blockchain are the most common for trust building. Security among healthcare users, and privacy. A system known as Blockchain-based Deep Learning as-a-Service (BinDaaS) is proposed for solving the discussed issues (Bhattacharya 2019). Telemedicine's most oriented application field is telesurgery that enables doctors to perform remotely real-time surgical procedures with the aid of an operating robots and a wireless communication network. To conduct high-quality surgery, it reduces long-distance traveling costs, time, and surgeon shortage. Security and privacy issues over the networks are solved in the study by implementing blockchain technology (Gupta 2019). The healthcare industry revolutionized from 1.0 to 4.0. 1.0 maintained patients record manually by the doctors and 2.0 has the redundancy issues. Likewise, 3.0 have no ability to deal with large amount of data. 4.0 handles all these problems easily (Hathaliya 2019, 2020).

Health IoT use cases can be broadly categorized in the following steps. Data from a randomized clinical trial of 357 patients seeking treatment for head and neck cancer were presented, the trial used a Bluetooth-enabled weight scale and blood pressure cuff to give patient physicians updates on symptoms and treatment responses every weekday. The patients who used this smart monitoring program, known as CYCORE, reported less serious cancer-related symptoms as opposed to a control group of patients who had routine weekly physician visits. The US Food and Drug Administration (FDA) approved Smart CGMs such as Ever sense and Freestyle Libre send blood glucose-level data to an iPhone, Android, or Apple Watch device, enabling the user to quickly test their details and spot patterns., a cognitive health assessment tool, partnered to discuss the use of an Apple Watch program to track and assess patients with Major Depressive Disorder (MDD) (Econsultancy 2019). Our motivation for this work is to sum-up all recent studies of data security schemes in one platform and perform their comparison analysis in terms of time, cost, and sensors memory range (Fig. 1).

Existing surveys provide an overview of data security in healthcare scenario (Shokeen 2019; Al-Janabi 2016) but we have focused on data security schemes in WBAN that mitigate various attacks to provide desired level of patients trust and satisfaction. We compared all the schemes with each other to appraise the most efficient schemes in terms of time, cost and memory consumption included in the study. The main contributions of our work are as follows.

1. To develop taxonomy covering security encryption techniques required for WBAN environment. In each part of the taxonomy, existing work has been discussed in detailed to handle several issues, such as preventing and predicting attacks on the network.
2. SLR is performed for very relevant schemes that focus on securing the healthcare data by mitigating security attacks while considering less memory consumption.

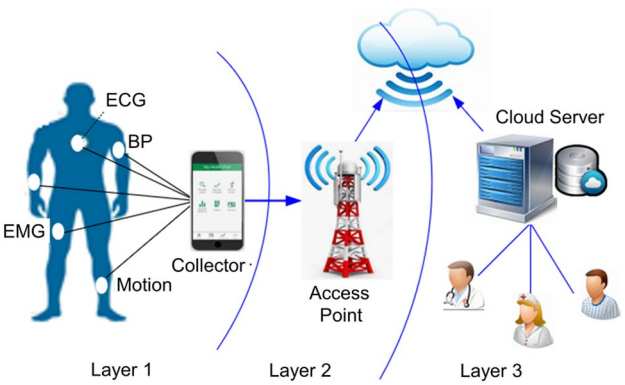

Fig. 1 WBAN architecture

3. Quality valuation is performed as per quality tests on each scheme to identify its linkage with research question.
4. Security analysis with the criticism is performed to motivate the researchers for giving efficient solutions to the problems.

The rest of the paper is arranged as follows. Section 1 presents the introduction to WBAN, Sect. 2 shows the Systematic literature review (SLR), Sect. 3 focused on the fact findings of the literature, Sect. 4 present security analysis and attacks evaluations. Section 5 explain discussion and future work. Section 6 conclude this work.

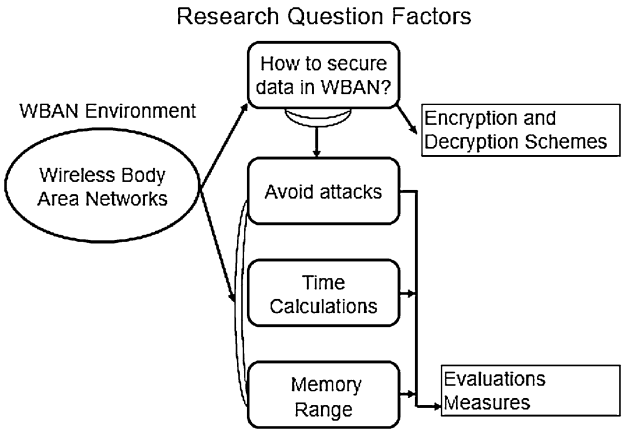

Fig. 2 Research questions factor

2 Systematic literature review

Systematic literature review (SLR) is a review that follows systematic tactics to gather subsidiary information. It supports to explore different classes of the present literature to a research question. It also emphasizes to explore the large quantity of existing literature for a research question or any field. It applies the prohibiting and inclusion criteria and exploring the literature gap for which an appropriate solution can be quantified. We also explored the guidelines is Paul (2019) and Menezes (2018).

2.1 Research question

The bottom line of research is to describe question which associate with the supreme purpose of the research. A research question articulates to prove that if there is present a data security algorithm which take lesser computational time.

Question: How to augment data security over WBAN from various attacks with time, cost, and less memory consumption?

Research Question reflects the core subject of the literature review and it simply explain the various security schemes against WBAN and categorize the multiple attacks that should be avoided by the multiple encryption schemes with less memory and time consumption. Second part of research question depicts bit deeper analysis of the literature review as depicted in Fig. 2.

2.2 Data redemption and digital libraries

A very vital step after explaining the research question is to design different phases that helps in exploring the present literature relevant to research question. By getting successful research, various steps are considered as follows; (i) acquire a full knowledge of research question, (ii) generate multiple string groups that can be utilize for the literature searching, (iii) employ various substitution of words, (iv) join diverse words to produce important expressions. This literature review based on the years 2016–2020 to get accurate results and to exclude irrelevant searches. Duplicate searches are also eliminated and make a reliable results Computerized Libraries utilized for searching the research articles. Precise words are used for searching the literature to reduce the risk of wrongly relevant inclusion. Some words used to study are: ((“Data security in WBAN” OR “Data Encryption in WBAN” OR “WBAN Security” OR “Homing Attack in WBAN” OR “Tempering Attack” AND (“ Secure medical data” OR data Protection” OR”data security through AES” OR “Secure data using digital signatures” OR “WBAN Cryptography).

Group of study is assembled by using included and forbidden merits as follows; (i) Included Merits: The research article is included if it fulfills the main four conditions. It should be relevant to the selected field of the literature and must be used keywords in the title. It also be noticed that they should be accessible easily from multiple digital libraries in form of PDF. The kind of research articles are also included if they compete the condition of years between 2016 and 2020 as recent studies. In order to include the paper in literature review, research questions demand must be satisfied by the articles as per following criteria; (a) research articles on WBAN’s data security, (b) research articles with accessible PDF, (c) research articles of year 2016–2020 (Recent Study) and (d) research articles that are applicable to research question. (ii) Forbidden Merits: articles are excluded from the literature review if they are getting duplicate. It also focused that considered research paper is inapplicable to the research question and mismatch the criteria of the questions. The research articles are not considered if they are not from the mentioning years. If the data security in WBAN not focused on the literature should also be excluded. Manuscript are forbidden as per following

criteria; (a) identical research articles, (b) inapplicable to research question, (c) research articles not between years 2016–2020, (d) research articles that emphasis on WBAN.

2.3 Quality estimation

This area indicates the prerequisites taken in thought with the end goal to choose an examination article. Hardly any quality tests are performed before the choice of any articles. The quality estimations are portrayed in Tables 1 and 2 demonstrates the assessment of each exploration article dependent on the estimations given in table. Filtration of the publications is done by following some rules and these rules have grading points accordingly. If the research papers are following routing protocols and detection systems, then this kind of publications have low priority as the literature should focused on the data security techniques. Some articles used privacy enhanced protocols which are not following the exact research questions demand but somehow privacy of data is focused therefore this type of research have ordinary priority. Research publications that are fully focused on data security and encryption/decryption techniques are appreciated and have higher priority. Quality costing of every article is based on following question:

Table 1 Priority estimation (PE)

Principles	PE
Routing protocol and detection system	×
Privacy enhanced protocols for WBAN	×
Security algorithm encryption/decryption	✓

Table 2 Prioritized articles

Research Paper	PE
BAN-trust: an attack-resilient malicious Node detection scheme for WBAN (Wenjia 2016)	×
Efficient high-rate key management for WBAN (Salehi 2016)	✓
Delay-aware optimization of physical layer security in multi-hop WBAN (Moosavi 2016)	×
A robust energy efficient and secure data dissemination protocol for WBAN (Prameela and Ponmuthuramalingam 2016)	×
Secure and energy-efficient data sharing on chaotic compressive sensing in body-to-body networks (Haipeng et al. 2017)	✓
Implementation of energy efficient/lightweight encryption algorithm for WBAN (Alshamsi 2017)	✓
Lightweight secure ECG transmission in WBAN—PRESENT Cipher Based Implementation (Narmadha 2017)	
Privacy based data communication for WBAN (Gowtham 2017)	×
Anonymous authentication with provable security (He 2017)	✓
Group-based cooperation on symmetric key generation (Li 2017)	✓
A secure three-party authentication protocol for WBAN (Vishwakarma and Mohapatra 2017)	×
Security issues and wearable sensors in WBAN (Sawaneh 2017)	×
Secure lightweight routing strategy for WBAN (Roy 2017)	×
An implementation of a lightweight end-to-end secured communication system for patient monitoring system (Chowdhury 2018)	✓
Secure data sharing using digital signatures (Anwar et al. 2018)	✓
WBAN security and privacy issue in e-healthcare (Malik et al.2018)	✓
Data storage mechanism based on blockchain with privacy protection in WBAN (Ren 2019)	✓
Biological key based security technique in WBAN (Rana 2019)	✓
Hybrid encryption algorithm in WBAN (Farooq 2018)	✓
Security framework for WBAN smart healthcare (Khan 2017)	✓
A survey on secure WBAN (Zou 2017)	✓
Data storage mechanism based on blockchain with privacy protection in WBAN (Ren et al. 2019)	✓
Hybrid encryption algorithm in WBAN (Farooq 2018)	✓
Energy efficient cluster formation and secure data outsourcing using TEOSCC and ECDH-IBT (Mukhtar 2016)	✓
Efficient and secure data delivery in software defined WBAN for virtual hospital (Shayokh 2016)	✓
BAN-trust: an attack-resilient malicious node detection (Li 2016)	×
Survey of main challenges (security and privacy) in WBAN (Al-Janabi 2016)	✓
Channel characteristic aware privacy protection mechanism (Zhang 2018)	✓
Group-based cooperation on symmetric key generation (Li 2017)	✓
Threats, challenges, security of WBAN using ZigBee (Tariq 2017)	×
A secure three-party authentication protocol for WBAN (Vishwakarma and Mohapatra 2017)	×
WBAN: attacks and countermeasures (Niksaz 2015)	×

Question: Does study focus on the data security in WBAN?

2.4 Research selection procedure

By describing the search material and fulfilling the possible standards, distinctive procedure is explored in Fig. 3. Following levels are considered; (i) Inceptive Level: At this level research articles are explored by employing specific phrases as discussed above. This is the initial phase for the assessment of the research which includes: (a) Research question, (b) Database libraries selection, (c) Included and forbidden merits, (d) Study Choices. (ii) Subservient Level: At this level, fact findings are chosen based on research question and these fact findings must satisfy the norms defined in Table 2. This is the execution of the inceptive level and consist of the systematic literature review composed of database search, study choices and data redemption analysis that fulfil the criteria of the research questions. Therefore, by focusing these points research papers of years between 2016 and 2020 are used in selection procedure. At this level, overall, 102 articles are considered. After searching relevant articles from multiple digital libraries, articles that fulfill the requirements of research questions are screened. Initially, 52 papers were shortlisted after studying, then the 25 pertinent articles are included in study which are fulfilling the criteria.

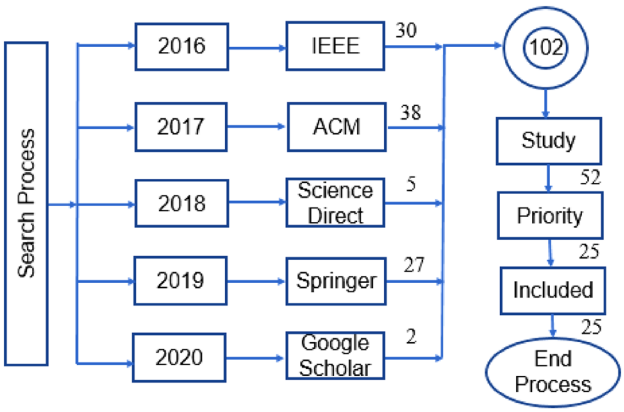

Fig. 3 Research selection process

3 Literature review

WBAN is a multifaceted network that involves various sort of sensor hubs that are utilized to detect and transmit information in various circumstances on real time basis. Sensors nodes gather important data and forward to the medical server for more analysis. Sensor hubs are extremely restricted in computational limits, memory, and power. Data contains very sensitive and vital information of patients, so the security and protection of the data is key task. There exist numerous assailants which can assault the very vital information of patients' health. The exploration of WBAN information security is cantered research around long stretches of 2016–2020. The quantity of articles considered are referred to table which gives a detail discussion of these contemplated articles. There are various measures of research finished to deal with information security in WBAN, and these examinations guarantee to work intensely in remote sensors arrange on various viewpoints. Multiple types of calculations are proposed for vanquished issues like conquering absence of intensity, inclusion issues and making restricted utilization of data transfer capacity. Literature is focuses on the different schemes like SHA (Secure hashing Algorithm), AES (Advanced Encryption Standards), LEA (Lightweight Encryption Cipher), Present Cipher and many other ciphers as illustrated in taxonomy of schemes in Fig. 4.

3.1 AES symmetric key based schemes

An energy efficient and secure protocol for WBAN (Gowtham 2017) [11], focuses on wearable device also called sensor devices are implanted into the body of patients to check the current situation of health. Human body is linked with internet through gateway devices. Medical specialists use this data to cure the patient's diseases like asthma, diabetes, heart attacks and blood pressures. An energy efficient and secure protocol for WBAN

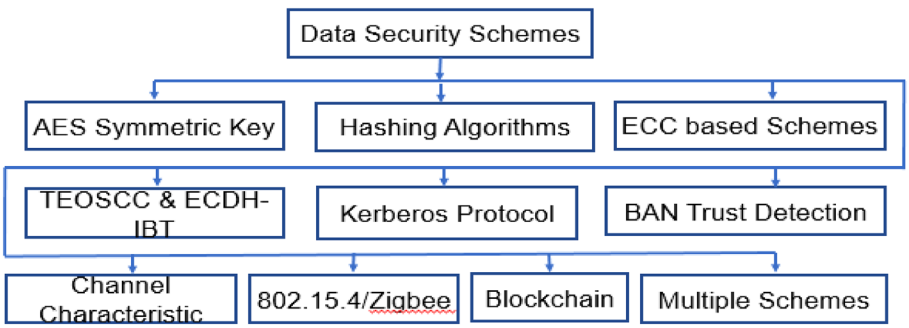

Fig. 4 Taxonomy of data security schemes

(Gowtham 2017) use Advanced encryption security (AES) based encryption and SHA-1 hash function is used to deliver the secure BAN. SHA-I is complex for WBAN, but complication is decreased by hash chain-based protocol which use chaos baker map for security. Sensor devices are well organized in memory space, computation control and bandwidth. (Gowtham 2017) protocol deploy chaos baker map to randomize the data and this technique is used to create the pseudorandom key streams.

Implementation of light weight End to End Secured Communication System for PMS (Li 2017) focuses on end to end secure transportation system for patient monitoring system. Patient's medical information is transmitted to the gateway from the sensor's device in the body through a wireless link. In this paper also focused on the data encryption to avoid data stealing and verification to make sure that only legitimate user is getting data. End to end secure PMS by focusing on the security of sensor to gateway wireless links with encryption protocol, also used (MQTT) telemetry transport protocol instead of hypertext transport protocol. AES is used for the encryption of the data and the encrypted data stored in the server from where a legitimate user can get the data for decryption and further actions. The advancement in (IoT) internet of things brings smart systems, such smart systems have wide scope in healthcare (Mukhtar 2016). Therefore, these systems are vulnerable to security and privacy. The secure framework implements low power and low resources. It uses AES-CTR mode to initialize counter value which some variable also called initial vector (IV) value which incremented through pseudorandom sequence. The size of the counter value depends upon encryption algorithm like AES-128 bits, it uses simple XOR operation as CTR mode used XOR operation.

WBAN needs lightweight and efficient resources to transmit data over the network (Prameela and Ponmuthuramalingam 2016). For security, many techniques are proposed, and this research article focused on the group-based cooperation on symmetric key creation through physical or link layer received signal strength indicator (RSSI) data collection is examined. This article proposed cooperative group solution to enhance the variation and size of RSSI data for efficiently key generation. The significant development is to utilize various channels between a member hub and a group or sometimes between two groups to randomly synthesize RSSI information with multi-overlap information thickness and improved information likeness and fluctuation. Likewise, a few bunch models are portrayed with the details of the protocol design. WBAN is linked with WSN (Al-Shamsi 2017) WBAN composed of tiny sensors that collects data from the human body and send it to biomedical sever through a network. The main purpose of the system is to ensure the security and confidentiality of the data over a network. Various security schemes are developed to ensure the security of the data and protect from multiple attacks. This article discusses cryptography and key management techniques to secure data. By providing strong cryptography and extensive calculations keeps the data secure. To use encryption technique for security time execution and memory consumption should be important to consider. Key management protocol is built up a protected application. These protocols are utilized to set up and circulate cryptographic keys to nodes in the networks. By and large, there are three kinds of key management protocol, confided in server, key pre distribution and self-authorizing Trusted server protocol depend on a confided in base station responsible for establishing the key agreement in the system network. It is viewed as that trusted server protocol are appropriate to networks in the environment of various resources.

WBAN is a developing technology that emphasis on the health examining system (E-consultancy 2019). It is very important to encrypt and decrypt healthcare information and it is also vital to generate the secrete keys at both source and destination side. Author proposed very useful technique to generate secret key, it is capable to generate 128 symmetric secret keys to secure the communication. WBAN consist of various nano sensors that measure the vital information of patients and it is critical to secure the WBAN link. Secure transmission through cryptographic techniques at wireless network protocol is important. Therefore, complex algorithms are used to encrypt the important data. High Rate Key Management Technique for WBAN focuses on RSS measurements of node A to node B are proposed (E-consultancy 2019). Communication between node A and node B guess their RSS measurements. It is capable to generate 128 symmetric secret keys to secure the communication. Results show that it generates symmetric secret keys with higher effects in both static and movement scenarios. Filtering process is implemented to decrease the bit mismatch before signal distortion passed to quantization process which is successful.

3.2 Hashing algorithm based schemes

Research reviews use Secure hashing algorithms (SHA) along with encryption techniques to make data transmission more secure and powerful (Anwar et al. 2018). By hash procedure, it generates digital signatures to transport patient's data in more secure and authentic way. This proposed algorithm used Asymmetric key generation approach which contains pair of public and private keys and this makes the algorithms slower and have high complexity. Securing Data Communication in WBAN with digital signatures (Anwar et al. 2018), proposed scheme is based on mixtures of different approaches by using secure keys and digital signatures for protecting data in WBAN. This scheme is very secure because of its arbitrary keys which are shared with

the BNC and the entire sensor node on the networks for encryption and decryption. BNC signs every data packet with SK by digital signatures and forward to all sensor's nodes in the networks. After validation by the BNC it sends to the medical server. D-sign used SHA-1 hash function to encrypt data into fix size bits known as hash values. Hash values and senders' keys generate digital signatures and then receiver used the sender's keys to decrypt the hash values. BNC compute the new hash values if these values are same it means data packet is not amended. In Gupta (2019), Chaos baker map focuses on a straightforward hash work convention together with Chaos Baker delineate which gives high secured information disclosure and spread. The body sensor hubs are source controlled regarding memory space, calculation control, data transmission and power. It uses 128 bits text and key sizes by utilizing hash function protocol. In view of controlled sources, computationally exorbitant and control concentrated procedures are not empowering for such hubs. Chaos Baker delineate is utilized to create the pseudorandom key streams. Every sensor hub gets the information and checks the information by utilizing the hash bind an incentive to decode the figure content. Chaotic sequence is pseudorandom, and finite is key matrix scheme and chaotic system create dimensions' matrices to form sequence. Sequence can be used as secret keys to encrypt or decrypt the patients' data. Chaotic compressive sensing is deployed in the body to body network.

3.3 Elliptic curve cryptography (ECC) based schemes

As the citizens are getting matured, it is very hard to satisfy the health fitness of seniors and patients by utilizing existing resources. Advancement in technology offers nano sensors that can be utilized around, just as implanted on human's body to gather health data, so the security of the data is very important. This article used ECC and Diffie Hallman (DH) to secure the data. There is vastly need of securing crucial data of patient's health, multiple schemes are used to secure the data (Rana 2019). Therefore, this paper used asymmetric algorithm ECC. DH is applied for the key generation into the system to get data security. There are two kinds of users including patients and doctors therefore this article also focused on the authentication of the users, to sign up the system users must store their personal information into the database like thumb or palm prints. This biological information then encrypted with ECC and DH algorithm. It is first converted into binary and then evaluated based on various key sizes like 128, 192 and 256 bits. The evaluation masseurs include encryption decryption time and key generation time.

WBAN is part of wireless sensor network in which small sensors are used to collect human's health data and forward it towards the hospital community (Farooq 2018). There is need to encrypt this data before transmitting it towards medical server to achieve security. That is why this article used hybrid encryption algorithm (HEA) for the security of data. HEA is used to encrypt and decrypt data where users must register themselves to get registration number and node ID. These numbers are used as a key a kept as a confidential. Then Elliptic curve Diffie Hellman is used to exchange these keys between sender and receiver. For encryption, this article used ECC 128 bit and AES 128 bits as a hybrid technique to secure the data. WBAN architecture consist of the intra WBAN and inter WBAN (Al-Janabi 2016). In intra WBAN the sensors around the patient's body use personal server (PS) as a gateway to transmit signal towards the next point while inter WBAN connects with main network through internet to retrieve patients' critical data of health. There is another very essential stage of WBAN that is beyond WBAN where database of the medical environment or biomedical server is placed. WBAN consist of very critical resources so the security and privacy are the main concern. Various data security techniques are proposed to secure the patients data. It presents ECC technique with very strong key management system to secure the data. It extracts the points on the curve to be used for cryptographic calculations. These points are unique to ensure more randomness of values. This technique used registration, verification, and key exchange methods to achieve the reliability and security of the data.

Rapid change in technology WBAN is a healthcare system that send data over a network (Vishwakarma and Mohapatra 2017). Transmission of data with security is a challenging task. This article used three party authentication protocol with ECC scheme for the security of the data. The research paper also used star topology for the WBAN. In asymmetric cryptography there are two types of keys are involved public key and private key which are related with each other mathematically. In cryptography there are two goals to achieve security for patient's data authentication and encryption. Public and private keys are used to encrypt/decrypt the sensitive data.

3.4 TEOSCC and ECDH-IBT

Different achievements in therapeutic innovative work have given the social insurance suppliers another assortment of instruments to improve the medicinal services (Mukhtar 2016). As a result, in future remote checking therapeutic frameworks known, as WBAN will turn out to be a piece of portable human services empowered with continuous checking. Security is the major issue in this type of environment therefore a proposed methodology based on clustering and encryption is presented. In clustering scheme, WBAN nodes are divided into various groups and these groups manages the data transmission. One of the selected groups of

nodes contain the cluster node as it is a cluster head, and the remaining nodes communicate around this cluster head. Cluster head connected with every node present in the group and it also maintain information and gather data from the cluster nodes and sends the data. Second scheme used in this article is encrypting the sensor data using ECDH Based Iterative Block Transformation (ECDH-IBT) algorithm.

3.5 Kerberos protocol

Rapid change in technology lead the idea of WBAN for smart healthcare system (Shayokh 2016). Therefore, high security for the sensitive data remains a main challenge. Multiple data security techniques are presented to secure the data, this article presents the software defined networking (SDN) layout for the data transmission and used networking authentication protocol names as Kerberos. This article shows flow chart for emergency data delivery which present that user will send an encapsulated data packet which is examined by the Kerberos protocol and give access to the legitimate user for getting data. For data transmission over the SDN, the SDN controller will examine the data format and suggest a specific route for data delivery.

3.6 BAN-trust detection

WBAN is a vital technology that support healthcare system (Li 2016). That is why security and reliability of the data is focus on this field. Various encryption and decryption techniques are proposed for the data security but still there is a chance of vulnerable to malevolent node attack. This article used BAN trust scheme to detect and cop with the malicious node attack in WBAN. BAN trusts consist of two parts one is the data analysis and the second is the trust management. It is not easy for WBAN's node to communicate directly but it is very important to transmit data therefore to understand either the node is trustworthy to interact or not, firstly check that if the node is ever interacted with any other node before then recommendations that it get from others are vital to evaluate the trustworthiness of that unknown node.

3.7 Channel characteristic

WBAN is the biomedical field which transmits very vital information of patient's health (Zhang 2018). The highly accessibility of resources may lead to tempering attack, malevolent node attack and injecting fake data attack. So, the protection of the data is the main issue in this environment. Multiple other techniques are proposed to secure the data, but this research article used a channel characteristic aware privacy protection mechanism for data security enhancement. In this paper encryption algorithms should follow firstly, that key used by two nodes have same sequence, second key have maximum size of 128 to 512 bit and the third is key should be used statistical randomness to encrypt data. Node authentication algorithm express the wireless channel to authenticate the authentic node-based correlation.

3.8 802.15.4/ZigBee

WBAN involves recent methodologies in medicinal recognizable proof, administration and as well as key design hinder for moving toward prompted systems (Tariq 2017). Remote BAN has a sufficiency to activity and familiarize modified works of fondness beat, movement, breath, physical temperature, sound, beating and claret pressure. In biomedical environment this kind of data should be secure against attackers and hackers. This article used ZigBee prerequisites of aegis are abstracts genuine, abstracts associate and embody introduction. It has 8 aegis levels, which canopy encryption and oath as well as gathered encryption and affidavit with deferent aegis angle in MAC layer. The aegis bandage of ZigBee does not acquiesce the two a great deal of key angles in symmetric-key cryptography: bearing and dispersion. The aegis associated accepted is so obscure, and it depends on which aegis angle is chosen, the uncertainty of the key being used. The 802.15.4 acknowledged works in three changed abundance groups for example 16 channels in the 2.4-GHz band, 10 channels in the 915-MHz band, and 1 approach in the 868-MHz band. These channels utilize the shortcut course of action advance range.

3.9 Blockchain

WBAN is a type of technology that is monitor and record human health signals for a long time (Ren 2019). As WBAN store and develop vital information of patients' health it raises different security and privacy concerns. To deal with the unauthorized access and with tempering the data blockchain technology and digital signatures are used. Blockchain is used to secure data from being tempered by involving chain of hash values to select the appropriate values used for encryption. On the other hand, digital signatures are used to as a verifier which means it ensures that data is accessible to administrators. Digital signatures also ensure mitigation of the non-repudiation attack by the users. The DVSSA signature technique used in this article make the size of the signatures in the blockchain are equals to the one-person signature size with the help of aggregation of all the persons' signature which reduce storage consumption greatly. The data of the users is signed through the DVSSA signature technique and then transmit the data for blockchain based calculations.

3.10 Multiple schemes

Another approach is used in the article is to secure physical layer (PHY) transmission (Farooq 2018). This method secure data encryption without need of the keys. Physical Layer Security In multi hop WBAN (Farooq 2018) MTFG (Multi Hop Topology formation Game) algorithm is used by the sensor nodes which coordinate with each other to make a tree topology for multi hop transmission in the uplink of the WBAN. This algorithm can be deployed in the distributed way and each sensor know about the existence of its neighbors to select the best path. Performance of the system is scrutinized in various scenarios and results reveal that the proposed scheme has best performance that can be adjusted according to the conflicting need of security and latency for multiple applications. The PRESENT Cipher Based Implementation (Hasan 2020) focuses on Block ciphers that are used to encrypt or decrypt the patient's data using 64 block text and 128 bits key. An algorithm is developed to get the QRT wave from ECG signal. This QRT wave differs according to patient's heart condition, as the normal heart signal has pre-defined value for the healthy person. Implementation is done in the MATLAB. ECG dataset can be reserved from MIT-BIH database. The structure of ECG signal gives P, Q, R, S, T, U amplitudes and intervals and they are the most common characteristics for the safe transmission within the WBAN. Block cipher PRESENT is used for the safety because it is more secure and lightweight. Security enhanced data communication protocol (Hathaliya 2019) that is Homomorphic encryption method is used to secure the sensitive data of the patients in 18 bytes text blocks. This encryption method performs specific computations on the plaintext and the ciphertext is generated. While decrypting the ciphertext by inversing it matches the plaintext of the algorithm. RSA is used for message padding bits. WBAN Security in E-Health presents (Roy 2017) BARI and distributed key management protocol based on biometric for the WBAN. This protocol gives security, confidentiality, and authentication to defend against different attacks and threats. It also presents protocol known as MAACE in which only legitimate users have right to get access of the sensitive data of the patients. This technique provides mutual authentication and access control depends on ECC. WBAN used to tiny sensors attached to the human body to collect data related to health of the patients (Al-said 2005). Then this data is transmitted towards the medical personnel through networks are through fixed channel. This transmission of data needs to be secured from the attackers. Multiple security schemes are used to encounter threats and challenges of WBAN. This article presents Biometric feature-based scheme which uses different recognition symbols or prints that can be used as a session key. This scheme is based on the Jules and Sudan (JS) algorithm. According to JS algorithms two communicating parties must be locked in polynomial value. Transmitter used this value to send secret data and if receiver want to acquire the data there is a need of reconstruction of the polynomial value.

WBAN is an area restricted sensor network where nodes can be placed on or inside the body (Salehi 2016). The main core of this field is to transfer data from node coordinator to medical server in an efficient manner. This article proposed priority aware protocol (PAP) to deal with smart healthcare system. PAP consists of mainly three units sensing, controller, and medical server units. The Sensing unit detects the information, allocates the dynamic priority to data packet based on estimated values and afterward dispatches it to the controller unit as per determined priority of the data packet. The controller unit sets an alarm flag as indicated by the priority of data packet and appropriately an alarm is created to the specialist as well as to the crisis contact. The unprecedented development of information and communication technologies in every sphere of life, especially in medical sectors, has given us more secure and seamless healthcare services (Sandhu 2020). The sector-based routing divides the network into multiple sectors with a sector head (SH) in each sector. The SH works as an SDESW where the SDN functionalities are implemented to retrieve control information from the controllers. Based on the control information, the SDESW routes the data packets to the appropriate destination. The SDESW is a static node which resides in the vicinity of the patient's bed or in a room (Sandhu 2020).

4 Security and attacks analysis

On the bases of research done on past years, it is viewed as that all the analysis can be investigated on the forthcoming security demands. While the greater part of the given methodologies keeps from various attacks and they still experience numerous. We have observed that key size 128 bits is used in He (2017), Hussein (2016), Roy (2017) and Shayokh (2016) as shown in Table 4. In Alshamsi (2017), Farooq (2018), Khan (2017), Mukhtar (2016) and Zhang (2018), key sizes large than 128 bits are also used to further strengthen the security level but it also increases the computation cost. It is also noticed that AES technique (Anwar et al. 2018; Prameela and Ponmuthuramalingam 2016; Chowdhury 2018) and RSSI (Salehi 2016; Li 2017) used 128 bits of sizes for data and keys avoided same types of attacks which are data eavesdropping and impairments attacks but implementation of both schemes are complex and have high memory usage. Security analysis of the literature is given in the Table 3 where multiple methodologies are studied along with possible attacks and criticism on these research schemes. It shows literature techniques that avoids various attacks. Some of the schemes avoid DOS type attacks and other focused to prevent Eavesdropping, Impersonation, and malevolent node attack. We have gathered multiple literature techniques to give an opportunity to create novel solutions

Table 3 Security analysis with criticism

Scheme	Plaintext/key size	Technique	Avoided attacks	Criticism
D-Sign (Anwar et al.2018), PMS (Chowdhury 2018) SHA-1 (Prameela and Ponmuthuramalingam 2016)	128 bits text/128, 192 and 256 bits (Anwar et al. 2018; Chowdhury 2018; Prameela and Ponmuthuramalingam 2016)	AES & MQTT (Anwar et al.2018; Prameela and Ponmuthuramalingam 2016; Chowdhury 2018)	Data eavesdropping Data impairment (Anwar et al. 2018; Chowdhury 2018; Prameela and Ponmuthuramalingam 2016)	Theoretical like file type attacks are effective (Alsaid 2005) Dos, IoT attacks not suitable for sensors networks (Chowdhury 2018), high Complexity (Prameela and Ponmuthuramalingam 2016)
Biometric (Malik et al.2018; Zou 2017)	N/A	Fingerprint or palm scanning, JS Algorithm (Zou 2017; Malik et al.2018)	Malevolent attacks (Malik et al.2018, Authentication (Zou 2017)	Complex and costly (Malik et al.2018), Multi-biometric key in the system also increases complexity in terms of storage, computations, power consumption, and execution time (Farooq 2018)
RSSI (Salehi, 2016; Li 2017)	128 symmetric KEYS (Salehi, 2016; Li 2017)	RSSI (Salehi, 2016; Li 2017)	Eavesdropping attacks (Salehi, 2016; Li 2017)	Complex algorithm, difficult to implement (Malik et al.2018), Large size key makes encryption complex. More time for decrypting data (Rana 2019)
PHY (Hussein 2016)	N/A	MTFG Algorithm	Delay Time attack	Make system slow (Malik et al.2018)
HASH Function (Prameela and Ponmuthuramalingam 2016)	128 bits	Chaos baker map	Malevolent Attacks	Complex dynamical behavior (Haipeng et al. 2017)
PCI (Narmadha 2017)	64 block text and 128 bits key	Cipher PRESENT-80	–	Short block size and large number of rounds which make the process of encryption slow (Malik et al.2018)
BBN (Haipeng et al. 2017)	N/A	Chaotic compressive sensing encryption	Impersonation attacks	Complex and long-distance distortion (Haipeng et al. 2017)
LEA (Alshamsi and Barka 2017)	128.192 and 256 key size and text size 128 bits	LEA	–	Vulnerable to new kind of cryptanalysis and data accuracy effects (Alshamsi and barka 2017)
SHE (Gowtham 2017)	18 bytes text size	Homomorphic encryption	Sinkhole attacks	This technique is risky because of connection (Malik et al.2018)
Blockchain (Ren 2019)	Size depends on aggregate of single person sign	DVSSA	Tempering and unauthorized access attack	Time consumption and complex (Ren 2019)
HEA (Farooq 2018) Counter Mode (Khan 2017) ECDH (Rana 2019)	128,192 and 256 bits (Farooq 2018; Khan 2017; Mukhtar 2016)	AES-CTR (Khan 2017) ECC and DDH (Rana and Kang 2019), ECC, AES (Farooq 2018)	Unauthorized access	AES and ECC are difficult to implement (Rani 2018). Complex, high processing, infeasible to implement (Khan 2017). ECDH make more complex exponentiation operation (Salehi 2016)
TEOSCC and ECDH-IBT (Mukhtar 2016)	–	TEOSCC and ECDH-IBT	–	Selection of cluster head is complex task and ECDH-IBT complex exponentiation operation (Mukhtar 2016; Salehi 2016)

Table 3 (continued)

Scheme	Plaintext/key size	Technique	Avoided attacks	Criticism
SDN (Shayokh, 2016; Hasan 2020)	–	Software defined	Authentication (Shayokh 2016)	Security vulnerabilities, inconsistency (Niksaz 2015). Network Complexity increases flow requests from SDESW (Hasan 2020)
RMDS (Li 2016)	–	BAN-Trust	Malicious node attack	Trusted server can be a single point (Niksaz 2015)
ECC (Al-Janabi 2016)	–	ECC	Authentication	Replay attack, insecure data communication (Anwar et al. 2018)
CCPP (Zhang 2018)	128–512 bits	Channel aware security mechanism	tempering, malevolent node attack	Authentication of each node is time consuming (Zhang 2018)
Survey (Tariq 2017)	–	802.15.4./ZigBee	–	ZIGBEE technology is commonly used with low speed (Ren 2019)
STA (Vishwakarma and Mohapatra 2017)	–	ECC	–	Asymmetric cryptography takes more processing time (Farooq 2018)
KM encryption (Niksaz 2015)	–	Key management	–	Malicious attackers can steal the key through wiretapping key exchange (Zhang 2018)
PAP (Sandhu 2020)	–	Priority aware protocol	–	Energy consumption increases with increase of priority (Sandhu 2020)

Table 4 Comparative analysis of techniques in terms of security (attacks, time)

Schemes	Impersonation	Eavesdropping	DOS	MN	Time
D-Sign (Anwar et al., 2018)	–	✓	–	–	✓
PMS (Chowdhury 2018)	–	–	–	–	✓
Biometric (Malik et al.2018;)	–	–	–	✓	–
SHA-1 (Prameela and Ponmuthuramalingam 2016)	–	–	–	✓	–
RSSI (Salehi 2016)	–	✓	–	–	–
MTFG (Hussein 2016)		–	✓	–	✓
Chaos Baker Map (Prameela and Ponmuthuramalingam 2016)	–	–	–	✓	–
Chaotic compression (Haipeng et al. 2017)	✓	–	–	–	–
LEA (Alshamsi 2017)	–	–	–	–	✓
Homomorphic (Gowtham 2017)	–	–	✓	–	✓
DVSSA (Ren 2019)	–	–	–	✓	–
ECC (Farooq 2018)	–	–	–	✓	–
JS algorithm (Zou 2017)	✓	–	–	–	–
TEOSCC and ECDH-IBT (Mukhtar 2016)	–	–	–	–	–
SDN (Shayokh 2016)	✓	–	–	–	–
BAN-Trust (Wenjia 2016)	–	–	–	✓	✓
802.15.4./ZIGBEE (Tariq 2017)	–	–	–	–	–
RSSI (Li 2017)	–	–	–	–	–
Channel aware security (Zhang 2018)	–	✓	–	✓	–

against possible attacks which are vulnerable to the schemes. Most of the research techniques have time and memory consumptions critics due to complex algorithms. AES (Anwar et al.2018) and ECC are difficult to implement on software in a manner of together safety and performance. It is also analyzed that some researchers used data security in concomitance of routing protocols. PMS (Chowdhury 2018) used combination of MQTT and AES in one scheme for data security. Table 4 explore the comparative analysis of different schemes in literature where the security is evaluated based on Impersonation, eavesdropping, DoS, Malicious nodes, and execution time. Several schemes in literature have covered these security measures to analyze the strengths for attack mitigation during the WBAN scenario.

Figure 5 shows the comparison of survey in the data security attacks make some research approaches fluster however some research approaches focuses on the strong data security communication. It explores the active attacks, greater computing attacks, more attacks on data and information as well that may interrupt the normal or emergency level of data exchange from sensing devices to central repositories.

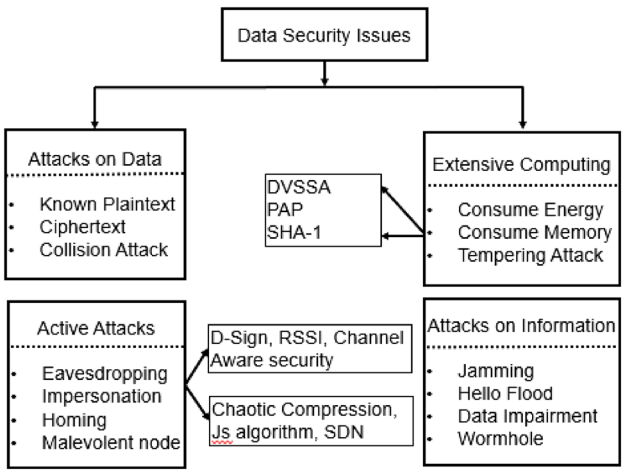

Fig. 5 Consequences and prompt

5 Discussion and future scope

In addition to the rising healthcare IoT sector, the COVID-19 pandemic has sparked debates about the future of IoT in healthcare, and how it can safely link healthcare professionals and patients. Hospitals and clinics were required to assess telehealth rapidly so that they could continue to treat certain patients without raising their risk of infection by placing them in treatment facilities. Hospitals are now continually under pressure to find ways of cutting costs. Wearable devices that allow certain patients to be treated and monitored at home may reduce the amount of resources required at the healthcare facility. Another technology that leads to IoT's future in healthcare is the implementation of 5 G networks, which offer broadband speeds 100 times faster than conventional 4 G networks. IoT devices rely on communication to communicate data

between patient and care provider and to transfer data. Quicker wireless data sharing allows IoT versatility in terms of the data volumes it can share and much quicker. For these changes, new healthcare IoT applications include devices to help patients stick to their medication at home; sleep monitoring devices that can track heart rate, oxygen levels and high-risk patient movements; remote temperature monitoring devices and continuous glucose monitoring sensors that attach to mobile devices and warn patients and clinicians to changes in blood sugar level. This latest pandemic experience combined with success and recent developments will boost IoT adoption and enable those who may otherwise have avoided the technology in the past to embark on it.

6 Conclusion

WBAN collects the vital signs of a patient and send it to any mobile device which is connected to a back-end servers and databases that can preserve a patient's records and provides relevant diagnostic recommendations. Multiple communication methodologies for a smart hospital using IoT system are extensively reviewed, while the vulnerabilities for security and privacy are highlighted. We have performed quality valuation to guarantee the connection of techniques with the research question. Since WBAN is a multifaceted field, few research approaches are considering to be reasonable. Different research approaches have demonstrated high security calculations, some are very complex and difficult. Though different other research techniques exhibited less security approaches which are fitting. This study has collected security key in WBAN after the investigation of numerous articles on recent years. This literature focuses about numerous information security approaches; and from all the exploration procedures, few are viewed as work superlative for information security. In literature, various existing techniques are observed to recognize how the security is upgraded for patients' health data.

References

Al-Janabi S, Al-Shourbaji I, Shojafar M, Shamshirband S (2016) Survey of main challenges (security and privacy) in wireless body area network for Healthcare Application. Egypt Inform J 18(2):113–122

Alsaid A, Mitchell CJ (2005) Dynamic content attacks on digital signatures. Inform Manag Comput Secur 13(4):328–336

Alshamsi AZ, Barka E (2017) Implementation of energy efficient/lightweight encryption algorithm for wireless body area networks. In: International Conference on Informatics, Health & Technology (ICIHT), p 7

Anwar M, Abdullah AH, Butt RA, Ashraf MW, Qureshi KN, Ullah F (2018) Securing data communication in wireless body area networks using digital signatures. Tech J Univ Eng Technol (UET) Taxila Pak 23(2):1–6

Bhattacharya P, Tanwar S, Bodkhe U, Tyagi S, Kumar N (2019) BinDaaS: blockchain-based deep-learning as-a-service in healthcare 4.0 applications. IEEE Trans 14:1

Chowdhury FS (2018) An implementation of a lightweight end-to-end secured communication system for patient monitoring system 5

Econsultancy (2019). The next decade may well see a revolution in the treatment and diagnosis of disease. Xeim, United Kingdom

Farooq S, Prashar D, Jyoti K (2018) Hybrid encryption algorithm in wireless body area network (WBAN). In: Rajesh S, Sushabhan C, Anita G (eds) Intelligent communication control and devices. Springer Nature, Singapore, p 10

Gowtham M (2017) Privacy enhanced data communication protocol for wireless body area network. In: International Conference on Advanced Computing and Communication Systems (ICACCS -2017), Coimbatore, India, p. 5

Gupta R, Tanwar S, Tyagi S, Kumar N, Obaidat MS, Sadoun B (2019). HaBiTs: Blockchain-based Telesurgery Framework for Healthcare 4.0. In: 2019 International Conference on Computer, Information and Telecommunication Systems (CITS). Beijing, China, 28–31 Aug 2019

Haipeng P, Ye T, Jurgen K, Lixiang L, Yixian Y, Daoshun W (2017) Secure and energy-efficient data transmission system based on chaotic compressive sensing in body-to-body networks. IEEE Trans Biomed Circuits Syst 11(3):16

Hasan K, Ahmed K, Biswas K, Islam MS, Sianaki OA (2020) Software-defined application-specific traffic management for wireless body area networks. Future Gener Comput Syst 107:274–285

Hathaliya J, Sharma P, Tanwar S, Gupta R (2019) Blockchain-based remote patient monitoring in healthcare 4.0. In: *2019* IEEE 9th International Conference on Advanced Computing (IACC). Tiruchirappalli, India, 13–14 Dec, 2019

Hathaliya JJ, Tanwar S (2020) An exhaustive survey on security and privacy issues in Healthcare 4.0. Comput Commun 153:311–335

He D, Zeadally S, Kumar N, Lee J-H (2017) Anonymous authentication for wireless body area networks with provable security. IEEE Syst J 11(4):1–12

Hussein M, Bui FM (2016) Delay-aware optimization of physical layer security in multi-hop wireless body area networks. IEEE Trans Inf Forensics Secur 9(4):13

Khan M, Jilani MT, Khan MK, Ahmed MB (2017) A security framework for wireless body area network based smart healthcare system. In: Conference: International Conference for Young Researchers in Informatics, Mathematics and Engineering, ICYRIME 2017, (p 6). 80–87

Kitchenham B, Brereton OP, Budgen D, Turner M, Bailey J, Linkman S (2008) Systematic literature reviews in software engineering—a systematic literature review. Inf Softw Technol 51(1):7–15

Li W, Zhu X (2016). BAN-Trust: an attack-resilient malicious node detection scheme for WBAN. In: International Conference on Computing, Networking and Communications (ICNC), (p. 5)

Li Z, Wang H, Fang H (2017) Group-based cooperation on symmetric key generation for wireless body area networks. IEEE Internet Things J 4(6):1955–1963

Malik MS, Ahmed M, Abdullah T, Kousar N, Shumaila MN (2018a) Wireless body area network security and privacy issue in e-healthcare. Int J Adv Comput Sci Appl 9(4):209–215

Menezes J, Gusmão C, Moura H (2018) Risk factors in software development projects: a systematic litrature review. Softw Qual J 1–26

Moosavi H, Bui FM (2016) Delay-aware optimization of physical layer security in multi-hop wireless body area networks. IEEE Trans Inf Forensics Secur 11(9):1928–1939

Mukhtar T, Chaudhary S (2016) Energy efficient cluster formation and secure data outsourcing using TEOSCC and ECDH-IBT technique in WBAN. In: International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), (p. 17). Chennai, India

Narmadha T, Kalaiarasi M, Meenakshi M (2017) Lightweight secure ECG transmission in wireless body area networks—PRESENT cipher based implementation. In: International Conference on Communication and Signal Processing,, (p. 5). India

Niksaz P (2015) Wireless body area networks: attacks and countermeasures. Int J Sci Eng Res 6(9):1–13

Okoli C, Schabram K (2010) A guide to conducting a systematic literature review of information system research. SSRN Electron J 10(43):879–210

Paul PC, Loane J, Regan G, McCaffery F (2019) Analysis of attacks and security requirements for wireless body area networks—a systematic literature review. In: Walker A., O'Connor R., Messnarz R. (eds) Systems, Software and Services Process Improvement. EuroSPI 2019. Communications in Computer and Information Science. Springer, Cham, pp 439–452

Prameela S, Ponmuthuramalingam P (2016) A robust energy efficient and secure data dissemination protocol for wireless body area networks. In: International Conference on Advances in Computer Applications (ICACA), 978-1-5090-3770-4/16/$31.00©2016 IEEE, p. 14. Coimbatore, India

Rana ES, Kang SS (2019) Implementation of biological key based security technique in wireless body area networks. Int J Innov Technol Explor Eng (IJITEE) 8(8):2156–2163

Rani C, Jagan L, Ch Harika L, Amara VD (2018) Light weight encryption algorithms for wireless body area network. Int J Eng Technol 7(2):64–66

Ren Y, Leng Y, Zhu F, Wang J, Kim H-J (2019) Data storage mechanism based on blockchain with privacy protection in wireless body area network. Sensors 19(10):2395

Roy M, Chowdhury C, Kundu A (2017) Secure lightweight routing (SLR) strategy for wireless body area networks. In: IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), (p. 4). Bhubaneswar, India

Salehi SA, Razzaque M, Tomeo-Reyes I, Hussain N, Kaviani V (2016) Efficient high-rate key management technique for wireless body area networks. In: 22nd Asia-Pacific Conference on Communications (APCC). Yogyakarta, Indonesia

Sandhu A, Malik A (2020) PAP: priority aware protocol for healthcare application in wireless body area network. Int J Recent Technol Eng (IJRTE) 8(5):7

Sawaneh IA, Sankoh I, Koroma DK (2017) A survey on security issues and wearable sensors in wireless body area network for healthcare system. In: 14th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), (p. 6). Chengdu, China

Shayokh MA, Abeshu A, Satrya G, Nugroho MA (2016) Efficient and secure data delivery in software defined WBAN for virtual hospital. In: International Conference on Control, Electronics, Renewable Energy and Communications (ICCEREC), (p. 5). Bandung, Indonesia

Shokeen S, Parkash D (2019) A systematic review of wireless body area network. In: International Conference on Automation, Computational and Technology Management (ICACTM), (p. 5). London, United Kingdom

Subbarayadu A, Radhika G, Vedhavathi R (2016) Survey secured data transmission from WBAN to sink. Int J Comput Sci Mob Comput 5(3):431–444

Tanwar S, Bhatia Q, Patel P, Kumari A, Singh PK, Hong WC (2019) Machine Learning Adoption In blockchain-Based Smart Applications: the challenges and a way forward. IEEE Access 4:474–488

Tariq MB, Abbas K (2017) Threats, challenges, security of wireless body area network (WBAN) using IEEE 802154/ZIGBEE. Int J Sci Eng 8(5):878–884

Vishwakarma R, Mohapatra RK (2017) A secure three-party authentication protocol for wireless body area networks. In: Third International Conference on Sensing, Signal Processing and Security (ICSSS), (p. 5). Chennai, India

Vora J, Nayyar A, Tanwar S, Tyagi S, Kumar N, Obaidat MS (2018) BHEEM: A blockchain-based framework for securing electronic health records. In: 2018 IEEE Globecom Workshops (GC Wkshps). Abu Dhabi, United Arab Emirates, 9–13 Dec. 2018

Wenjia, L., & Xianshu, Z. (2016). BAN-Trust: An Attack-Resilient Malicious Node. *2016 International Conference on Computing, Networking and Communications, Communications and Information Security*, (p. 5). Kauai, HI, USA .

Wohlin, C. (may 2014). Guidelines for Snowballing in Systematic Literature Studies and a Replication in Software Engineering. *EASE '14: Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering*, (pp. 1–10). Sweden.

Zhang P, Ma J (2018) Channel characteristic aware privacy protection mechanism in WBAN. Sensors 18(8):2403

Zou S (2017) A survey on secure wireless body area networks. Secur Communi Net 2017:1–9