International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 03 | March - 2022 ISSN: 2582-3930

A Survey on Wireless Body Area Network : Characterstics , Architecture , Challenges.

Er Simranjit kaur *,Er Mamta

Department of Computer Science and Engineering, DAV University , Jalandhar, India

ABSTRACT

People have benefited from the recent advancement and spread of new techniques in a variety of ways. Most importantly, this has become increasingly linked to healthcare information exchange digital services. Remote patient monitoring is among the most important services, since it allows healthcare professionals to check, assess, and treat people without needing to be personally there. Biosensors that have been miniaturised have the advantage of being able to be implanted in, on, or off the bodies of individuals, and then they can relay physiologic data via wireless to cloud computers. This technique is known as a Wireless Body Area Network. This paper discusses WBAN architecture, WBAN telecommunication, WBAN impediments, and many other aspects of WBAN. WBAN faces a variety of challenges in terms of obtaining a high standard of security because because of its resource constraints and critical applications. This paper presents a comprehensive review of WBAN technologies, focusing on confidentiality as well as upcoming study objectives.

Keywords: Survey, Authentication; Security; Wireless Body Area Network

1. INTRODUCTION

A Wireless Body Area Network is a wireless network consisting of a collection of small bio-medical units positioned on the body's surface, beneath the epidermis, within the body, or in close enough proximity towards the body. WBAN is defined by IEEE 802.15.6 , which was published in 2012, is the only WBAN benchmark available. IEEE 802.15.6 is a secured, short-range connectivity system that supports a wide variety of data rates to meet the needs of a variety of purposes. The ultra-low-power detectors can check the body's key physiological signs and, sometimes in cases, can even administer a medication straight into the body.

Both wearable and implantable medical equipment are designed to transmit true bio-signal information to the server or device on the network [1]. Based on the node category, the observed data could include body temperature, blood pressure, respiration measurement, heart rate, blood glucose level, Electrocardiogram, or Electromyogram. In the aged and those with chronic health conditions, tracking these physiologic

indicators allows them more mobility and freedom, and also the capacity to intervene promptly when necessary. The world's older population is quickly growing at present. In th United Kingdom, the number of people aged 85 and over will have doubled by mid-2041.

Furthermore, the World Health Organization estimates that by 2030, diabetes will be among the leading causes of death, with diabetic care paying for up to 15% of the overall government healthcare expenditure. As a consequence, overall health expenditure and the proportion of medical personnel who are stressed are projected to skyrocket. This encourages the use of WBAN's latest innovations to enhance patient quality of life, enhance standard operating procedures, make timely intervention choices, and cut total health-care costs while also lowering healthcare staff's long hours at work. WBAN's importance and importance in medical systems promotes the standardization effort, which allows multiple solutions from different providers to connect with each other.

IEEE, 2012 defines WBAN's Physical and Medium Access Control layers. IEEE Task Group 6 has opted to be using three type of physical layering to adapt to diverse applications due to the increasing standards of WBAN transponders, such as battery performance. These physical layers are summed up as follows by the authors in [2]:

•NB PHY: seven distinct carrier frequencies with varying data speeds are supported.

•UWB PHY: supports two frequency bands, higher and lower, each one with a variable range of channels but same bandwidth. The design of the UWB PHY enables a long-term deployment with minimal complication and power consumption.

•Human body communication (HBC) PHY: provides a single low-frequency band with a centre frequency of 21 MHz, wherein data is transferred via the body of the patient using Electric Field Communication technology.

The below is a summary of the layout of the paper. The section two gives some basic information on WBAN design features. Section 3 describes the WBAN topology, whereas Section 4 describes the WBAN communication architecture. The literature evaluation of existing WBAN studies is explained in Section 5. WBAN's security and privacy policies are outlined in section 6. The last remarks are found in Section 7.

2. WBAN design characteristics

The IEEE 802.15.6 specification [3] has the important overall design features:

•The network can be restored in the case of a connection or node loss.

•The able to manage a wide variety of data rates, from tens of Kilobits per second to nearly 10 Mb / s, in order to meet the requirements of all potential applications;

•Ensures trustworthy transmission for healthcare and non-medical purposes with appropriate jitter and latency levels

•Provides effective power usage technique that enables the low-power sources to last for many years.

•Ability to use security measures such as authorization, cryptography, and authenticity.

•Allows both in-body as well as on sensor nodes to cohabit.

•The ability to add and remove nodes in a timely manner.

•Allows for operation in a diverse wireless channel.

•It meets the standards for Specific Absorption Rate.

•Supports scaling upto 64 nodes.

3. WBAN topology

A conceptual set of sensors and a singular hub is described as a Body Area Network. It employs a star topology and two communication mechanisms: basic one-hop and enhanced two-hop. Nodes interchange frame instantly with the BAN hub in a basic one-hop star structure, however in an enhanced two-hop design, a relay node is available, and nodes can interact either straightforwardly with the hub or via relay node, as seen in Fig. 1. The overall nodes in a single BAN is specified by the MAC sublayer variable mMaxBAN- Size, that has been fixed to 64. Depending on their functionality, BAN nodes can be classified into various groups [4]:

•Hub: The names hub, sink, and coordinator all refer to a certain type of node. Several BANs and external networks can join to the hub through it. The BAN, and any external communications, are under its control. It has higher resources as contrasted to certain BAN nodes.

•Relay node: A few nodes can carry information between the hub and the end nodes. They are inside the hub's direct transmission range. Relaying is required by WBAN's expanded star topology.

•End node: It refers to all other nodes.

They are designed to do specific tasks, such as enabling communication directly with the hub if they really are within direct transmission range, or through relay nodes when they're not.

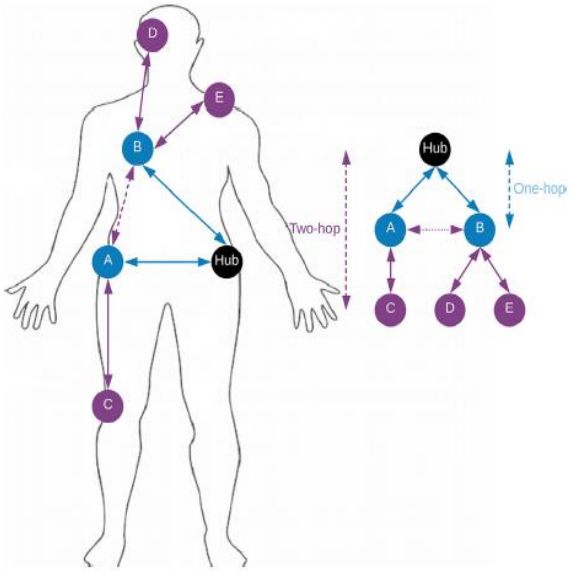

Fig 1: Topology of WBAN

4. WBAN communication architecture

When evaluating the complete WBAN ecosystem, exchange of information can be broken down into many tiers. The authors of [6] divided interaction between nano-nodes and micro-nodes into 4 levels to ensure to examine it. The WBAN protocol, on the other hand, defines 3 levels of interaction:

•Intra-BAN connectivity at Tier 1: Interaction among sensor nodes as well as between sensor nodes as well as the hub is the initial rung of data transfer. The broadcaster and recipient are both within body range in this level of interaction. Sensors that are in-body, on-body, and off-body are all covered. The sensor node's qualities, and the physical layer and frequencies used, define the data flow.

•Tier-2 Inter-BAN communication: It involves interactions between different BANs and also communication between both the hub and the Access Points.

•Tier-3 Communication Beyond the BAN: it refers to all conversations that take place outside of the BAN. Tier 3 is where the Access points and the healthcare servers communicate via the web. All of the mechanisms used here are defined by the TCP/IP layer. Figure 2 depicts all WBAN connectivity layers.

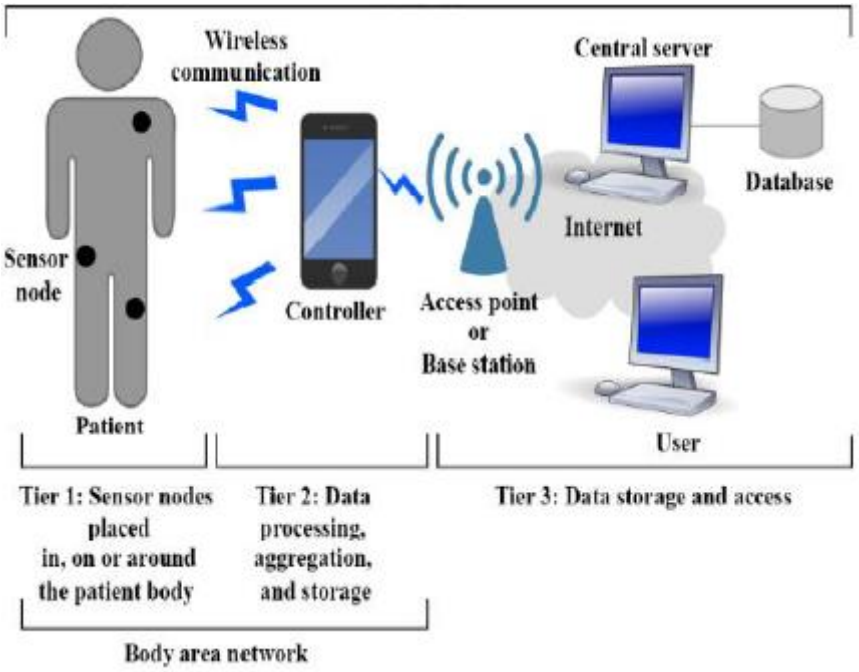

Fig 2 : WBAN Architecture

5. Security in WBAN

Data protection and confidentiality are important factors in all types of networks. WBAN processes critical information that, if interfered with, could endanger clients' wellness or even their survival, necessitating more important security measures to safeguard clients from all sorts of hostile activity. Regardless of the fact that safety is a top concern in WBAN, there are many other unknown areas due to WBAN's source limits, and a broad range of confidentiality concerns acquired from Wsns. To establish a sufficient standard of security in WBAN, authenticity at every tier of interaction should be ensured. The WBAN's basic safety standards are as follows [7]:

•Confidentiality: Information must be safeguarded from unauthorised access both during transfer of data. WBAN data comprises very confidential health information about a patient. If it's kept in a simple form as well as the node is hacked during communication on an open line by eavesdropping, or whether it's saved in a simple format and the node is attacked, it could be disclosed. As a result, selecting an effective encryption technique to conceal data is critical [8].

•Integrity: When receiving data, the recipient party must ensure the data is authentic but has never been interfered with it during transfer. By stealing data during transmission and inserting, removing, or changing the sent message, data is easily manipulated. Privacy protections are ineffective.

•Data Availability: An opponent can jeopardise availability of data and prohibit permitted parties from accessing it. Barring connection between caregivers and sensor nodes could jeopardise the persons life due to the critical implementations of WBAN. As a consequence, for this application system, maintaining the ability to access crucial data in any circumstance is critical [10].

•Data Authentication: Unlike data integrity, which works to avoid data from being altered during transfer, data validation aims to verify that the message conveyed came from the originating node, which is assumed to be the message's provider. IEEE 802.15.6 defines the Message Authentication Code, which is used to check that the received message was sent by the originator [11].

•Data Freshness: The adversaries may attempt to catch and play transmitted signals, leading WBAN to become confused and unstable. As a corollary, a technique must be implemented to check that the information received is recent and that no opponent is recreating old posts. Freshness guarantees that received communications are in sequence and completed on time, but it does not ensure that they will be delivered as promised [12].

•Secure Management: Many safety approaches, such as cryptography, decoding, and data verification, need key exchange protocol, that must be done safely. Safety at tier-3 of transmission has garnered considerable attention in the research [13] since it is an ubiquitous tier connecting heterogeneous networks, although numerous research possibilities remain at tiers 1 and 2.

Security characteristics

•Level-0 Unsecured Communication: No safeguards are used at this degree of security. Data are sent unsecured frames because they lack confidentiality, identification, authenticity validation, or replaying prevention.

•Level-1 Authentication: messages are sent in encrypted authorized blocks, assuring message validity, replay resistance, and consistency validation. However, there have been no measures in place to make sure that information is kept private and secret.

•*Level-2 Authentication and Encryption*: The high degree of protection recommended in the guideline. Data encryption and authorized frames are used to send and receive messages. As a corollary, anonymity, message legitimacy, fidelity, and replayed avoidance are all guaranteed at this level of security. Nodes and hubs must identify the suitable level of security during affiliation process based on their needs. Figure 3 shows the security framework that is used to generate keys and provide services [14].

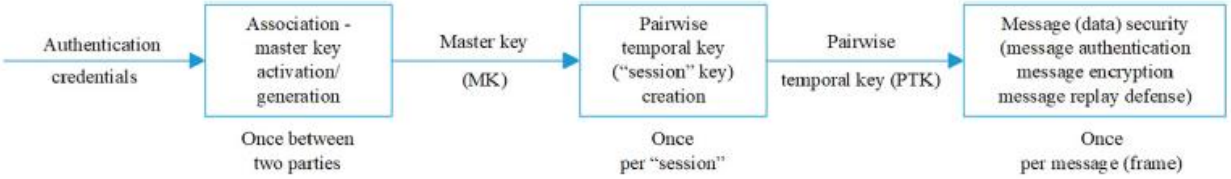

Fig 3: security keys

6. LITERATURE REVIEW

In [20] Venkatasubramanian et al. presented a key agreement, fuzzy vault, and a biometric-based privacy strategy which all are part of the current PSKA concept for WBAN. It allows neighbouring sensors in a WBAN to agree on a symmetrical encryption key in a secure manner, reducing the need to key information before deployment. Despite the fact that PSKA is an energy based technology derived from humans, it necessitates increased computational time. It also prevents an attacker from exploiting the critical details because no pre-deployment is required. PSKA emphasises on physiological characteristics to provide safe inter-sensor connections. To lock and unlock, PSKA uses a fuzzy vault.

In [21], Li et al. describe a hybrid biometric-based access control solution that includes key creation, delivery, and governance as well as low-power cryptosystem. In this identifier technique, keys are also generated from physiological signs such as Electrocardiogram data. The vital signs from the person's blood are securely captured and transmitted. In this method, the information packet is encoded using the AES and DES methods. All through the key production and transmission phases, the IPI transmitter binary encoding is employed to create a secret key.

Ali and Khan discuss a safe intersensor transmission key agreement method based on the Discrete Wavelet Transform in their paper [22]. (DWT). In this technology, the EKG data is used to produce encryption keys for inter-sensor interactions. The iris or fingerprint properties are used to lock and then release the modules during an interchange phase among connecting sensors, with the locking and releasing done using watermarking. The block must be sealed when a watermark is provided to the transmitter and the block is released. The watermark is then removed on the recipient's end. The two most crucial steps in this strategy are feature generation and key agreement.

In their paper [23], AL-Rassan et al. proposed an ECG-based key management technique for WBANs that produces keys based on human biological factors. This technology uses biochemical parameters and pre-loading processes to ensure the safe inter-sensor connectivity in WBANs. After gathering ECG characteristics from physiological measurements, the key establishment phase is utilised to constructed the keys. Before the installation of pre-distribution in the suggested ECG based technique, a key pool with a large key size is loaded into to the sensor network from a key bank and an unique key to every sensor.

In [26], Ali and Khan present a key management and consensus method that allows WBAN sensor nodes to decide on a shared secret key with the private server. This solution defends WBANs from selectively forward, denial of service, and replaying threats by providing a reply authentication mechanism across nodes. The proposed method uses the ECG signal to generate a secure key. The values communicated are a portion of the feature attributes formed by the person's ECG signal's peak intensities.

ETRES [27] is yet another likelihood-based TMS that uses the exponentially probabilistic model to describe a node's reputational value, assuming comparable future actions. LTMS [31] is a compact and light global medical sensor network. Two ways for determining the trust level are suggested in LTMS to fit source constraints of in-body, on-body, and off-body sensor nodes. In terms of attack detection and processor cost, LTMS surpassed well-known trust control strategies such as ReTrust [33] and RaRTrust [34].

The scholars Toorani [16] looked at the primary agreement processes for MK setup in the WBAN specification. He believes that four key-establishing mechanisms in the norm are susceptible to Key Compromises, Online frauds, and thus failure to reach the forward secrecy condition. Offline dictionary attacks are also possible with one of the methods. A pre - shared Master Key should be enabled or formed between both the hub as well as every node during in the connection process in order to ensure secure connectionless communication, and a Pair wise Temporal Key should be created and exchanged between both parties to be used in each conversation.

[17] acknowledged the use of WBAN in the health and non-medical domains, and a detailed assessment of the PHY and MAC layers. The paper also offered valuable information on a variety of routing algorithms and safety, and a number of technological implementation challenges. A Group Temporal Key is created in the hub for safe multicast transmission and then distributed with the applicable multicast members of the group by the hub. Regardless of the fact that the IEEE 802.15.6 benchmark provides three level of protection, current study shows that the standard's security procedures are still prone to a range of attacks.

Alam et al. [18] describe a new use of WBAN wearables for protection and critical applications in challenging situations like oil and gas refinery and diverse petroleum industry. Inter-WBAN exchanges are depicted in this architecture, in which the WBAN supervisor serves as a versatile device that remotely links body sensors to exterior network devices via WiFi or Broadband cellular networks such as GSM, GPRS, 3G, and LTE..

A contrast of several WBAN techniques and new challenges is offered in this work [19]. Moreover, with some case reports based on factual installations and experimenting in the fields and computations, the paper will focus on radio channel analysis, energy usage reduction, and cohabitation challenges in WBAN. The investigation of cohabitation issues and disturbance reduction approaches is provided in WBAN technology [18]. In addition, simulated results and quantitative depictions of compatibility considerations are examined among IEEE 802.15.6, IEEE 802.15.4, and low-power WiFi systems. The section also covers solutions for interference management, as well as a modeling approach and specifications.

The link among WBAN and cognitive radio technology is demonstrated in this research [16]. The Mac protocol, application server, and obstacles are all explored for context - aware applications. In this paper, the vulnerabilities in WBAN for smart healthcare are thoroughly investigated. Based on the recent literature review, various types of dialogues are presented, with a focus on only a few clinical uses and associated systems for WBAN.

In [15], the researchers explain a short survey just on home setting of a WBAN-based digital healthcare system, which demonstrates the development of a typical example in a community home and the acceptance of mobile phone smart healthcare. It presents WBAN frameworks and focuses on energy-saving routing techniques. The report also includes the use of virtual reality as a new conception of WBAN, and the integration of WBAN with cognitive radio system for energy saving.

7. CONCLUSION

WBAN is a growing subject of study in a variety of fields. This paper examines previous WBAN studies as well as recent work on a variety of topics. WBANs are networks of tiny sensors installed within, upon, and around the body that can be used for a variety of purposes. Because WBANs handle sensitive data on

a regular basis, ensuring safety in such networks is critical. As a consequence, various cutting-edge security solutions were created in the research that employs a variety of technologies to safeguard the confidentiality and protection of existence data. A review of current research on WBANs as well as future research directions are offered in this survey article. First, a brief explanation of the WBAN architecture, topology, and design criteria was presented. Security requirements have also been looked into. Finally, possible re-search directions and opportunities have been suggested.

REFERENCES

[1] Fushan Wei, P. Vijayakumar , Jian Shen , Ruijie Zhang and Li Li, "A provably secure password-based anonymous authentication scheme for wireless body area networks," *International Journal of Computers and Electrical Engineering*, vol. 65, pp. 322-331, April 2017.

[2] Maryam el Azhari, Ahmed Toumanari, Rachid Latif and Nadya el Moussaid, "Relay Based Thermal Aware and Mobility Support Routing Protocol for Wireless Body Sensor Networks," *International Journal of Communication Networks and Information Security (IJCNIS)*, vol. 8, no. 2, pp. 64-73, August 2016.

[3] Maged Hamada Ibrahim, Saru Kumari, Ashok Kumar Das, Mohammad Wazid and Vanga Odelu, "Secure anonymous mutual authentication forstar two-tier wireless body area networks," *International Jornal of computer methods and programs in bio medicine*, vol. 135, pp. 37-50, July 2016.

[4] Shikha Pathania and Naveen Bilandi, "Security Issues In Wireless Body Area Network," *International Journal of Computer Science and Mobile Computing*, vol. 3, no. 4, pp. 1171-1178, April 2014.

[5] Sourav Sinha, Neeraj Kumar Goyal, Rajib Mall,, "Early prediction of reliability and availability of combined hardware-software systems based on functional failures,," *Journal of Systems Architecture*, vol. 92, pp. 23-38, 2019.

[6] Shihong Zou, Yanhong Xu, Honggang Wang, Zhouzhou Li, Shanzhi Chen and Bo Hu, "A Survey on Secure Wireless Body Area Networks," *International Journal of Security and Communication Networks*, vol. 2017, p. 9, March 2017.

[7] Marisol García-Valls, Abhishek Dubey, Vicent Botti,, "Introducing the new paradigm of Social Dispersed Computing: Applications, Technologies and Challenges," *Journal of Systems Architecture*, vol. 91, pp. 83-102, 2018.

[8] Gautam M. Borkar and Anjali R. Mahajan, "Security Aware Dual Authentication based Routing Scheme using Fuzzy Logic with Secure data Dissemination for Mobile Ad-hoc Networks," *International Journal of Applied Security Research*, vol. 13, no. 2, pp. 223-249, March 2018.

[9] Prosanta Gope and Tzonelih Hwang, "BSN-Care: A Secure IoT-based Modern Healthcare System Using Body Sensor Network," *IEEE Sensors Journal* , vol. 16, no. 5, pp. 1368-1376, March 2016.

[10] Kunal M pattani and Palak J Chauhan, "Spin Protocol For Wireless Sensor Network," *International Journal of Advance Research inEngineering, Science & Technology(IJAREST)*, vol. 2, no. 5, pp. 1-3, May 2015.

[11] Geethapriya Thamilarasu, "iDetect: an intelligent intrusion detection system for wireless body area networks," *International Journal of Security and Networks* , vol. 11, no. 1-2, pp. 82-93, March 2016.

[12] Megha Gupta, "Hybrid Intrusion Detection System: Technology and Development ," *International Journal of Computer Applications*, vol.115, no. 9, pp. 5-8, April 2015.

[13] Kajal Rai and M. Shyamala Devi, "Intrusion Detection Systems: A Review," *Journal of Network and Information Security*, vol. 1, no. 2,December 2013.

[14] Ibrahim Ghafir, Martin Husak and Vaclav Prenosil, "A Survey on Intrusion Detection and Prevention Systems," *International Conferenceon Student Conference Zvůle 2014, IEEE/UREL*, August, 2014.

[15] Mohammad Masdari , Safiyyeh Ahmadzadeh and Moazam Bidaki, "Key Management in Wireless Body Area Network:Challenges and Issues," *Journal of Network and Computer Applications*, vol. 91, no. 1, pp. 36-51, August 2017.

[16] Tan Jin and Wang Yijing, "The Research of Secure Transport Protocol Based on Node's Clock Characteristics for Body Area Networks," *International Journal of Security and Its Aplications* , vol. 8, no. 5, pp. 457-470, 2014.39

[17] Qiuyan lin, Woongryul leon, Changwhan Lee, Youngchul Choi and Dongho Woni, "Fingerprint-based user authentication scheme for," in *Fifth International Conference on Ubiquitous and Future Networks (ICUFN)*, Da Nang, Vietnam, July, 2013, pp. 178-183.

[18] Emna Kalai Zaghouani, Adel Benzina and Rabah Attia, "ECG based authentication for e-healthcare systems: Towards a secured ECG features transmission," in *13th International Wireless Communications and Mobile Computing Conference (IWCMC)*, Valencia, Spain,June, 2017.

[19] Rollin McCraty and Fred Shaffer, "Heart Rate Variability: New Perspectives on Physiological Mechanisms, Assessment of Selfregulatory Capacity, and Health Risk," *Global Advances In Health And Medicine*, vol. 4, no. 1, pp. 46-61, January 2015.

[20] Tilendra Choudhary and M. Sabarimalai Manikandan, "Robust Photoplethysmographic (PPG) Based Biometric Authentication for Wireless Body Area Networks and m-Health Applications," in *Twenty Second National Conference on Communication (NCC)*, Guwahati, India, March, 2016.

[21] M. Anwar , A. H. Abdullah, R. A. Butt, M. W. Ashraf, K. N. Qureshi and F. Ullah, "Securing Data Communication in Wireless Body Area Networks Using Digital Signatures," *Technical Journal*, vol. 23, no. 2, pp. 50-55, August 2018.

[22] Zakia El uahhab and Hanan El bakkali, "Calculating and Evaluating Trustworthiness of," *International Journal of Communication Networks and Information Security (IJCNIS)*, vol. 8, no. 3, pp. 136-146, December 2016.

[23] Mohsen Toorani, "Cryptanalysis of Two PAKE Protocols for Body Area Networks and Smart Environments ," *International Journal of Network Security*, vol. 17, no. 5, pp. 629-636, September 2015.

[24] Ms. I.Shanmugapriya and Dr. K.Karthikeyan, "Reputation based Incentive Scheme for Secured Data Privacy in Wireless Body Area Network Communication," *International Journal of Advances in Computational Sciences and Technology*, vol. 10, no. 7, pp. 2095-2117,2017.

[25] Pradeep Kumar and Anand Sharma, "Survey on Authentication Process in Body Area Network," *International Journal of Electronics Engineering Research*, vol. 9, no. 6, pp. 913-921, 2017.

[26] Jie Zhang, Xin Huang, Paul Craig, Alan Marshall and Dawei Liu, "An Improved Protocol for the Password Authenticated Association of IEEE 802.15.6 Standard that Alleviates Computational Burden on the Node," *Symmetry*, vol. 8, no. 11, November 2016.

[27] Muhammad Khurram Khan and Saru Kumari, "An Improved User Authentication Protocol for Healthcare Services via Wireless Medical Sensor Networks," *International Journal of Distributed Sensor Networks*, vol. 10, no. 4, pp. 1-10, April 2014.

[28] Junghyun Nam, Kim-Kwang Raymond Choo, Sangchul Han, Moonseong Kim,Juryon Paik and Dongho Won, "Efficient and Anonymous Two-Factor User Authentication in Wireless Sensor Networks: Achieving User Anonymity with Lightweight Sensor Computation," *Plos One*, vol. 10, no. 4, pp. 1-21, April 2015.

[29] Seulgi Shin, Sung Woon Lee and Hyunsung Kim, "Authentication Protocol for Healthcare Services over Wireless Body Area Networks," *International Journal of Computer and Communication Engineering*, vol. 5, no. 1, pp. 50-61, January 2016.

[30] Sang Guun Yoo, "Cryptanalysis of Several Authentication Schemes forHealthcare Applications Using Wireless Medical Sensor Networks," in *ICNCC '16 Proceedings of the Fifth International Conference on Network, Communication and Computing*, Kyoto, Japan,Decemebr, 2016, pp. 282-286.