EFFICIENT IOT BASED WBAN USING NOVEL ENERGY CLOSENESS BASED ROUTING MECHANISMS

Vijaya Karthik S V
Research Scholar, Anna University, Chennai.
Mob: +91 – 9443344434, E-Mail : visitvijay88@gmail.com

ABSTRACT

Wireless Body Area Networks (WBAN) is defined as an emerging and a necessity solution to fulfil the needs of remote health related issues and remote monitoring of the health parameters. The health related datas from the elderly persons or the patients can be passed to the medical server and thereby the medical data can be monitored by the doctor remotely and providing the required medical prescriptions. In this WBAN, while transferring the data, the security is an important parameter to be considered and the priority of the data to be transferred is on high consideration as the data is related to medical field. There are variety of challenges that have been faced with the data transfer from patient to the medical server and the data transfer from doctor to the patient. To the overcome those challenges, the cache prediction and replacement algorithm for maximizing the cache utilization is proposed in this research. Also, the hash code computation technique is adopted to have the trustworthy of data. i.e., for the security of data transfer between the servers. At last, energy based efficient routing for the data transmission, energy closeness-based routing algorithm is suggested in this research.

Keywords: Wireless Body Area Network (WBAN), Security, Energy closeness-based Routing, Hash code Computation, Distributed Key arrangement.

INTRODUCTION

Wireless Communication has shown several merits to our society. This communication is made possible that use the recent technologies with the assistance of 4G, 5G, LTE and many others. In recent years, M2M – machine to machine communication has been a desired field for research. In addition, communication amongst human and machines has been the next target. T.G Zimmerman introduced a PAN (Personal Area Network). A lightweight, low-power, and small physiological sensors made it probable to associate them for forming BAN-Body Area Network. This association is complemented by wireless technology. Thus, Wireless Body Area Network (WBAN) is built. This network signifies the natural union amongst miniaturization and connectivity. WBAN consists of various sensors which sample, progress as well as communicate essential signs such as blood pressure, heartbeat rate and oxygen saturation.

The similar process can be performed for environmental metrics like temperature, location, light, and humidity. These sensors are attached within the dresses or with the body. More focus is attained for implantation of these sensors within the body [1].

In WBAN, the communication network can be partitioned into two parts. The first one indicates the communication amongst sensors. An architecture (three-tier) is accepted upon by implanting an additional communication layer amongst WBAN co-ordinator and sink node or WBAN gateway.

Thus, the IoT (Internet of Things) and WBAN possess a unified future. IoT is the modern promising field to study and is evolving as a platform where smart objects have an internet connection to receive and transmit data. IoT persists to grow as many devices connected to it keeps increasing. A WBAN might be utilized with technologies that rely on IoT to monitor human-body.

In healthcare, an accurately presented WBAN coupled with new IoT based devices can inform physicians about the criticality and condition of the patients in advance leading to enhanced quality for life. In addition, heterogeneous WBANs based on IoT will bring modifications in healthcare in near future. This technology is believed to bring effective modifications in the medical field. The necessary data corresponding to medicine is sensed through small power sensors. This is later forwarded to destination nodes where physicians take needed actions based on sensed data. In addition, WBAN is an enhancement in technology. Its use to treat humans is a boon. It is integrated with IoT-technology [2].

Additionally, the BAN – Body Area Network is evolving as favourable wireless network's technology and widely deployed in the medical application field for storage, data extraction as well as transmission of details about the customized health-care facilities. The inter-sensor communication security within Body Area Networks is dangerous in protecting the privacy of health data and to assure secure healthcare delivery.

The increasing use of WCN (Wireless Communication Networks) as well as the constant electrical device shrinking have provided the WBANs development. This article [3] explained the several authentication strategies and protocols accessible for WBAN. This study also afforded a study of authentication protocols corresponding to multi-level for WBANs. This article also itemized the design challenges in the authentication protocols of WBAN.

The results of this study afforded necessary future path for further study on the progress of WBANs. Thus, this paper afforded an overall view on the exhibited research challenges. It affords the way for upcoming study in the authentication protocols area for BANs.

The health industry is a particular domain for employment of IoT (Internet of Things) based technologies. Many researches have been implemented in the health industry to reduce the resource utilization and thus enhance the efficacy. The utilization of IoT integrated with additional technologies brought quality progression in the health-sector at reduced cost.

WBANs is one equivalent technology that will aid patients extremely in the forthcoming and will create a high productivity as it will eradicate the need to stay at hospital or home for a prolonged period. IoT and WBAN possess a combined future. This is because WBANs is a set of heterogeneous devices that is based on sensor.

For better combination of WBANs and IoT, various limitations restricting their combination must be solved. One such issue is the effective routing of data in restricted RSNs (Resource Sensor Nodes) in WBANs. Hence to resolve this, the study [4] proposed a EHCRP – Energy Harvested and Cooperative enabled effective Routing Protocol) for IoT-WBAN has been introduced.

In addition, the proposed methodology has been intended to solve additional issues like restricted network lifetime, duplicate sensed-data transmission and so on. The introduced protocol takes various WBAN parameters for effective routing that include SN-Sink Node's residual energy, hop-count to reach sink, levels of node congestion, SNR (Signal-to-Noise Ratio) and accessible network bandwidth. Path-cost evaluation function has been computed to choose forwarder node by utilizing these metrics.

The effective utilization of path-cost evaluation process led to efficient multi-hop data routing and enhanced the efficiency and reliability of data transmission in the network. Simulation has been carried out to validate the efficacy of the introduced technique. The simulation results exhibited that using proposed methodology there has been an increase in network throughput, and lifetime thereby minimizing end to end delay.

Moreover, WBAN is a particular vital component in the evolving IoT and it can monitor vital behavioural and physiological user information via wearable sensors providing an innovative paradigm for the succeeding generation of health-care systems.

Nevertheless, due to intrinsic open WC features, privacy, and security challenges for communication of WBANs remain unsolved. Hence this study [5] proposed a secure group-key management and biometric authentication for WBAN. This article adopted a novel communication infrastructure for WBAN. The distinct physiological ECG (Electrocardiogram) characteristics for user has been positioned in authentication. Then, effective group-key management including the legitimate sensors has been explored.

Here minimum computation cost is needed for dynamic updation of key in sensor side. Analysis of security represents that the introduced authentication strategy can accomplish desired security features and afford resistance towards several attacks. The performance of the proposed technique is analysed to evaluate its efficacy. The results attained from performance analysis represent that the introduced technique is effective and efficient when compared to traditional WBAN authentication strategies.

LITERATURE REVIEW

This section describes the reviews of various existing works related to efficient system to provide security in WBAN as well as to perform efficient routing. Moreover, in this article [6] an application for CL-PDA (Cross Layer-Protocol Design Architecture) of ECDSA (Elliptic Curve Digital Signature Algorithm) is introduced.

Simulation is performed using NS-2. The results explored the efficiency of the system with respect to throughput, packet delivery, and delay and so on.

In addition, this study [7] introduced a protocol that utilize innovative cluster-head selection method named as EBMADM (Energy Budget based Multiple Attributes Decision Making) strategy. It has been found that the proposed method enhanced network lifetime, throughput, and stability. Real-time implementation is yet to be done which is a drawback.

In the same way, this paper [8] introduced a Wi-Fi module and a set of wearable sensor assisted transmission which permits the remote monitoring execution of several health related metrics. Simulation is carried out which exhibited effective results.

In addition, this article [9] utilized co-operative transmission amongst IoT sensor nodes for e-health applications to improve the wireless communication security with respect to secrecy capacity by considering the devices that are resource-enhanced. The results showed the efficiency of the proposed methodology.

Moreover, this study [10] explored the outline of wearable sensors to track physical and physiological alterations in day-to-day life, applications as well as their basics. The systems that rely on wearable sensors possess many abilities to be exhibited as well as predict the technological advancement providing the transformation of the way in which healthcare will appear in near future. This study highlights the importance of localization in BAN. It also affords an overview about validating the localization system's performance. It also explored the various kinds of techniques and sensors for fusing the data produced by sensors.

Additionally, this paper [11] formulated a transmission strategy that is energy effective followed by MDP (Markov Decision Process) that efficiently finds the actions to be implemented explained with respect to gaining ideal transmission power for communication of intra-BAN. Simulation has been carried out to assess the efficiency of the proposed system which revealed effective outcomes. More dimensions have to be included in strategy formulation which is a drawback.

In addition, this study [12] intended to provide two security schemes for WBAN. The experimental results explored better outcome while using proposed method. On contrary, WBAN protocols based on block-chain are essential to afford privacy and security of sensitive information.

Hence this study [13] proposed a CLAKA (Certificate Less Authenticated Key Agreement) for WBAN protocol that rely on block-chain. In addition, a session-key has been established amongst block-chain node and Personal Digital Assistant (PDA) to ensure secure communication. A key agreement that has been authenticated for WBAN that rely on block-chain accomplished more security characteristics than traditional system. A blind signature has also been presented amongst block-chain nodes to afford nodes anonymity as well as to verify the node's eligibility. The introduced CLAKA is safe in Read Only Memory. It is appropriate for WBANs and is lightweight for devices that have low capability. A heterogeneous key agreement and authentication must be designed in near future for block-chain that rely on WBANs.

Similarly, this study [14] introduced an innovative CLAKA protocol based for pairing for WBANs that rely on block-chain. The proposed CLAKA has been compared with other methods. The comparative analysis explored that the proposed method in block-chain environment affords high security characteristics than traditional methods. The introduced technique also evades failure and hence manages the overall system. The proposed methodology is evaluated which exhibited that the recommended system is effective and appropriate for WBANs. Heterogeneous CLAKA must be designed for WBANs that rely on block-chain so as to present an authenticated key-agreement scheme amongst certificate-less cryptosystem and PKI. Thus, in WBAN, the sensor devices transfer the collected human data (physiological) to the local node through a public channel. Prior to data-transmission, the local node and sensor device must accomplish key agreement and mutual authentication.

Hence, this study [15] introduced a safe mutual authentication strategy in WBANs that rely on block-chain. An informal and formal security analysis has been utilized to examine the security of this strategy. Subsequently, a comparative analysis has been undertaken with respect to communication and computation costs. The results obtained from comparative analysis explored that the introduced strategy explore high efficiency control in terms of energy consumption. Moreover, WBAN is susceptible to several kinds of attacks as the information of patients sensed by devices are confidential and sensitive. The WBAN has been an existing healthcare application. Thus, it is vital to assure that the information sensed by sensors of WBAN is secured and free from unauthorized users. A strong authentication and security solutions are required to achieve secured WBANs. The investigators suggested various authentication schemes and security solutions over the past few decades. Nevertheless, the lack of cohesive study in authentication and security do not provide high goal of affording a bird-eye vision of the field.

To satisfy the aims as given above, this study [16] provided various survey of the necessities for security, threats, attackers as well as the present solutions with clear security mechanism classification in WBANs. This study also discussed about the authentication schemes, its design as well as its classification. Moreover, this article provided an overview of the applications, challenges, and recommendations for further authentication techniques of WBANs. This research also expanded the WBAN functionality, its building blocks, its technologies as well as a clear-cut view of WBAN with respect to authentication and security.

In addition, WSN (Wireless Sensor Networks) have been utilized widely with the growth of sensor devices, the WBANs are typical applications in WSNs. the human body's physiological data is collected via the wearable sensors and these data is stored in the server. WBANs are vulnerable to many attacks due to dynamic nature of the network devices and the opened. The centralized architecture (two-hops) comprises of one hub. Thus, in the hub-node, the data is stored which might be destroyed by attackers. If the attackers conquer the node, overall network will get paralyzed.

This study [17] recommended a WBANs architecture that rely on block-chain. Here the blind-signature and authentication protocol amongst nodes have been designed in innovative WBANs model creating the data transmission more reliable and secured. Experiments have been carried out to assess the efficacy of the introduced method. The empirical outcomes exhibited that the recommended technique is reliable. It also explored high safety and stability level when compared to state-of-the-art methods. The system must be enhanced in a way that it can store huge quantity of data thereby increasing security. It is a drawback of this article which needs to be rectified soon.

Moreover, this paper [18] introduced OPOT-Optimum Path Optimum Temperature. This technique reduced the temperature impact on sensor-node through setting of threshold limits which aids in choosing ideal routing path, uniform heat distribution among network sensors. The information of neighbour nodes such as distance and temperature amongst source and sink have been computed prior to fixing a communication path. When the distance amongst source and sink is high, then the relay-node is chosen, and data transmission is performed via this node. When the destination node corresponds to neighbouring node, then data transmission is performed in a direct way. The data signals that are sensed have been allocated with a priority level as critical data-high priority, normal data-low priority and abnormal data medium-priority. When the temperature of node is minimum than threshold value, then the data signals will be transmitted in a particular order. This ensures that critical data of patients has been reached on time. The recommended methodology has been compared with the traditional methods and the outcomes explored that the introduced protocol enhanced the performance with respect to power, delay, energy as well as network lifetime when compared to state-of-the-art methods.

Accordingly, WBAN can efficiently alter the lifestyle and health monitoring where numerous body metrics are measured by using sensor devices (bio-medical). Conversely, reliability and power consumption are the challenges in WBAN. CC-Cooperative Communication typically expand the WBAN's network lifetime and permits reliable data packet delivery. Thus this study [19] intended to introduce CEPRAN – Co-operative Energy-efficient and Priority-based-Reliable-routing protocol to increase the energy efficacy and reliability of WBAN by utilizing Co-operative communication technique. Initially, a CSO (Cuckoo Search Optimization) technique has been introduced to detect a relay-node from a collection of sensor nodes. Subsequently, NS-3 simulator has been used to execute CEPRAN. The simulation results exhibited that the proposed methodology outperformed other traditional methods. This article has to be expanded with mobility conditions. Several QoS (Quality of Service) parameters must be examined. In addition, the testing of protocol in real-time must be performed.

In contrary, chronic patients have been supported by WBAN and they are adapting to this developing health-care system. A medical data is not regular all the times. Thus, the desire for critical data is predicted to be maximum, the security need also become vital. Hence this paper [20] addressed HMS – Healthcare Monitoring System which adopted a certain standard for WBAN. In addition, a modified-version of MAC has been proposed to predict residual energy and datatypes on body-sensors. Thus, an enhanced HMS has been proposed for data transmission that is aware of delay to perform key-distribution, data aggregation, data classification and channel selection. Here a smartphone serves as a coordinator which collects data from WBAN on data receiving, it finds the effective channel from accessible multiple inputs to ensure data transmission. Lastly, a hybrid NBNN (Naïve Bayesian Neural Network) has been utilized to monitor servers which perform data classification. Simulation has been performed and the results showed improved performance with respect to throughput, delay, security, packet loss and accuracy.

Additionally, this study [21] applied the routing code of critical-data for transmitting related data from the node in inner body to on-body MSS (Medical Super Sensor) nodes. In this article MSS serves as controller which can manage every injected sensor inside the person's body as their member. When the sensor node of inner body is identifying any physical actions from human body, it compares that data with level of threshold value stored prior to that of sensor node. When sensors attain high deviation in their outcomes, it follows CDR (Critical Data Routing) for transmission till it reaches the rest mode.

Simulation has been carried out on MATLAB which showed the results with respect to network lifespan, efficiency of throughput, energy spending. Moreover, this study [22] introduced ESR-W (Energy-efficient and SDN based Routing) with the utilization of Dijkstra algorithm based on fuzzy. The most suitable route determination has been performed with reactive and central scheme among many users of SD-WBAN. Battery level, SNR and number of hops are the parameters utilized to make decisions for routing. Numerous simulations have been implemented to compare the existing and proposed methodology in accordance with delay, energy consumption, and throughput and packet transmission rate. Security has to be considered and it is a drawback.

RESEARCH GAP

- The performance of the system that is the security in WBAN will degrade when it undergoes huge count of collisions. Hence in this study, the security in WBAN is increased through the proposed technique irrespective of the number of collisions.
- Key distribution can be heavy in large environments. Thus, in this study, distributed key agreement strategy is proposed to avoid the cumbersome of key-distribution in large environments.
- It is uncertain whether the data will reach the destination and it is not effective for node distribution of high-density. Thus, this article proposed novel cache prediction and replacement algorithm, hash code computation to find if IoT entries trust one another, distributed key agreement approach for session key agreement and energy closeness based routing method and accomplished optimized energy efficiency, enhanced security, throughput and network lifetime thereby minimizing packet loss.

Problem Identification

- Efficiency of WBAN is vital in all IoT based applications. The challenges to evolving technologies enhances with its progression and time.
- The WBAN faced various challenges that are categorized into six divisions. They are mobility, energy, communications, security, QoS and networking. It is shown in the Figure 1.
- The major issue is security which needs to be solved. The energy harvesting method is a solution for power issue. Energy harvesting can eradicate the charging of batteries either partial or full based on the method. WBAN's security architecture is challenging than any other networks. Scalability, efficiency as well as usability are the necessities for security architecture corresponding to WBAN.
- The public key infrastructure shows several challenges related with storage, revocation and certificates certification and it can be solved by the distributed session keys.

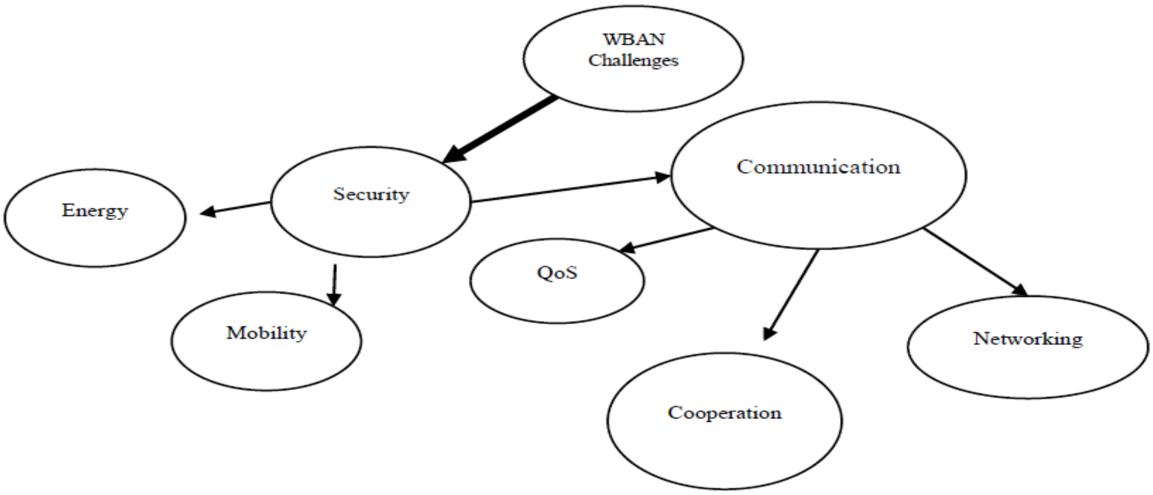

Figure.1. Taxonomy of security challenges in WBAN

OBJECTIVE

The following are the objectives of the proposed study,

- To implement the cache prediction and replacement algorithm for maximizing the cache utility after the deployment of sensor nodes.
- To perform the trust value evaluation and distributing the several data, hash code computation is implemented.
- To perform the session key agreement using the trusted third party, distributed key agreement approach utilized.
- To perform the efficient routing for the data transmission without loss, energy closeness-based routing method is implemented.

RESEARCH DESIGN- METHODOLOGY

In IoT based W-BAN networks, the body sensor nodes are deployed initially. Then the caches are predicted based on the cache prediction and replacement algorithm. The nodes are sending multiple data and it is splitted as distributed multiple data. Several data are distributed and trust value evaluated using the hash code computation. Further the block-chain is obtained to store the session keys based on distributed key agreement approach.

This approach used for performing the session key agreement. If the key's validation time is over then it is obtained from the base station. Using the new energy closeness-based routing method, data transmission routing is performed. Finally, the performance analysis is evaluated for the newly developed study. The overall flow of the proposed study is shown in following figure.2.

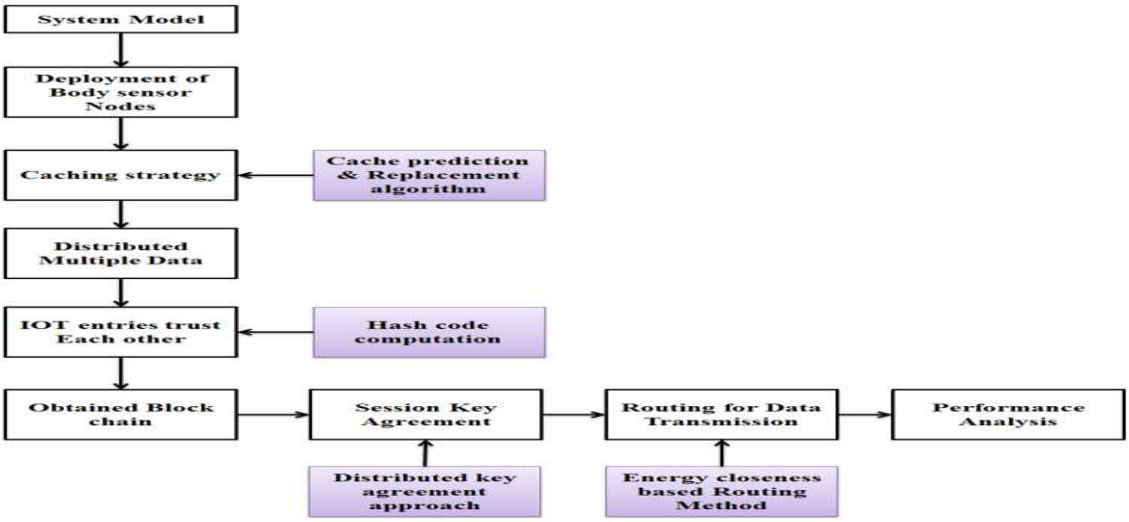
System Model
Deployment of Body sensor Nodes
Caching strategy
Cache prediction & Replacement algorithm
Distributed Multiple Data
IOT entries trust Each other
Hash code computation
Obtained Block chain
Session Key Agreement
Routing for Data Transmission
Performance Analysis
Distributed key agreement approach
Energy closeness based Routing Method

Figure.2. Overall Proposed Flow

The proposed innovative technologies are described as, the cache prediction and replacement algorithm considered as initial new concept, highlights the numerous homogeneous cache allocating mechanisms. To maximize the cache utility, partial caching is explored through this technique and the whole content is divided into portions which have been cached independently or else explored the chunks common properties of similar contents.

The multiple data are distributed, and trust value evaluated using the hash computation. To ensure the data integrity, hash function is involved. Timestamps are added in which the hashing verified that it is valid message. To the nodes all hash blocks are spread, and similar ledgers are mutually kept. For verification, the ledgers are made public. The user’s public keys are utilized to check if it is altered or not.

Another approach namely distributed key agreement approach utilized the public and private keys. The relationship among the private key’s authority public key and public key are guaranteed by the traditional public key infrastructure (PKI). However, the PKI shows several challenges related with storage, revocation, and certificates certification. This issue is sorted out by this proposed approach with the trusted third party to create a communication channel. Initially the secured session key generated for the secure connection among the dual users for secure connection establishment using the trusted third party which significantly perform the session key distribution. This approach is mainly for two users and not shared the session key which is secured.

Finally, the routing is performed by the energy closeness-based routing method, the sensor nodes position changed often because of the human body mobility. Similarly, the consumption of power is insignificant and its lesser related with transmission of data packet. For network lifetime prolongation, the sensor nodes are harvest the energy based on the proposed approach.

For the distance among the sink node and sensor node the Euclidean distance formula is utilized, and the path loss is also considered in this study.

POSSIBLE OUTCOMES

The proposed study is evaluated in terms of various performance analysis such as accuracy in data transmission, packet ratio, security, energy consumption and so on. Effective results are expected while comparing it with the existing approaches utilizing the IoT based W-BAN network.

REFERENCES

1) M. T. Arefin, M. H. Ali, and A. F. Haque, "Wireless body area network: An overview and various applications," Journal of Computer and Communications, vol. 5, pp. 53-64, 2017.
2) G. Cai, Y. Fang, J. Wen, G. Han, and X. Yang, "QoS-aware buffer-aided relaying implant WBAN for healthcare IoT: Opportunities and challenges," IEEE Network, vol. 33, pp. 96-103, 2019.
3) A. Joshi and A. K. Mohapatra, "Authentication protocols for wireless body area network with key management approach," Journal of Discrete Mathematical Sciences and Cryptography, vol. 22, pp. 219-240, 2019.
4) M. D. Khan, Z. Ullah, A. Ahmad, B. Hayat, A. Almogren, K. H. Kim, et al., "Energy harvested and cooperative enabled efficient routing protocol (EHCRP) for IoT-WBAN," Sensors, vol. 20, p. 6267, 2020.
5) H. Tan and I. Chung, "Secure authentication and group key distribution scheme for WBANs based on smartphone ECG sensor," IEEE Access, vol. 7, pp. 151459-151474, 2019.
6) P. Sharavanan, D. Sridharan, and R. Kumar, "A privacy preservation secure cross layer protocol design for IoT based Wireless Body Area Networks Using ECDSA Framework," Journal of medical systems, vol. 42, pp. 1-11, 2018.
7) A. Choudhary, M. Nizamuddin, M. K. Singh, and V. K. Sachan, "Energy budget based multiple attribute decision making (EB-MADM) algorithm for cooperative clustering in wireless body area networks," Journal of Electrical Engineering & Technology, vol. 14, pp. 421-433, 2019.
8) M. G. Annapoorani, P. Inja, P. Medhi, V. Thapliyal, and M. S. Kaushik, "Healthcare Monitoring in IOT using WBAN," 2018.
9) A. Arfaoui, A. Kribeche, and S. M. Senouci, "Cooperative MIMO for Adaptive Physical Layer Security in WBAN," in ICC 2020-2020 IEEE International Conference on Communications (ICC), 2020, pp. 1-7.

10) T. Poongodi, A. Rathee, R. Indrakumari, and P. Suresh, "IoT sensing capabilities: sensor deployment and node discovery, wearable sensors, wireless body area network (WBAN), data acquisition," in Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm, ed: Springer, 2020, pp. 127-151.
11) M. Roy, C. Chowdhury, and N. Aslam, "Designing transmission strategies for enhancing communications in medical IoT using Markov decision process," Sensors, vol. 18, p. 4450, 2018.
12) F. H. Khan, R. Shams, H. H. Rizvi, and F. Qazi, "A secure crypto base authentication and communication suite in Wireless Body Area Network (WBAN) for IoT applications," Wireless Personal Communications, vol. 103, pp. 2877-2890, 2018.
13) G. Mwitende, I. Ali, N. Eltayieb, B. Wang, and F. Li, "Authenticated key agreement for blockchain-based WBAN," Telecommunication Systems, vol. 74, pp. 347-365, 2020.
14) G. Mwitende, Y. Ye, I. Ali, and F. Li, "Certificateless authenticated key agreement for blockchain-based WBANs," Journal of Systems Architecture, vol. 110, p. 101777, 2020.
15) J. Xu, X. Meng, W. Liang, H. Zhou, and K.-C. Li, "A secure mutual authentication scheme of blockchain-based in WBANs," China Communications, vol. 17, pp. 34-49, 2020.
16) B. Narwal and A. K. Mohapatra, "A Survey on security and authentication in Wireless Body Area Networks," Journal of Systems Architecture, p. 101883, 2020.
17) L. Xiao, D. Han, X. Meng, W. Liang, and K.-C. Li, "A Secure Framework for Data Sharing in Private Blockchain-Based WBANs," IEEE Access, vol. 8, pp. 153956-153968, 2020.
18) B. Banuselvasaraswathy and V. Rathinasabapathy, "Self-heat controlling energy efficient OPOT routing protocol for WBAN," Wireless Networks, pp. 1-12, 2020.
19) M. Geetha and R. Ganesan, "CEPRAN-Cooperative Energy Efficient and Priority Based Reliable Routing Protocol with Network Coding for WBAN," Wireless Personal Communications, pp. 1-19, 2020.
20) A. H. Sharmila and N. Jaisankar, "E-MHMS: enhanced MAC-based secure delay-aware healthcare monitoring system in WBAN," Cluster Computing, vol. 23, pp. 1725-1740, 2020.
21) A. K. Sagar, S. Singh, and A. Kumar, "Energy-aware WBAN for health monitoring using critical data routing (CDR)," Wireless Personal Communications, pp. 1-30, 2020.
22) M. Cicioğlu and A. Çalhan, "Energy-efficient and SDN-enabled routing algorithm for wireless body area networks," Computer Communications, vol. 160, pp. 228-239, 2020.

Biography of the Author

Vijaya Karthik S V (corresponding author) was born in India. He received his Bachelor of Engineering in Electronics and Communication Engineering from Anna University in the year of 2009 and Master of Engineering in Embedded and Real Time Systems from Anna University in the year of 2011. He has published more than 10 Papers in various International Journals.