*January-February 2020*
*ISSN: 0193-4120 Page No. 15832 - 15838*

# Privacy Preserved Healthcare System for Wireless Body Area Networks

**Damanpreet Kaur,** Department of Computer Science Engineering, University Institute of Engineering, Chandigarh University, Mohali, Punjab (INDIA), damanpreetk898@gmail.com
**Ruchika Gupta,** Department of Computer Science Engineering, University Institute of Engineering, Chandigarh University, Mohali, Punjab (INDIA), ruchikae7396@cumail.in

***Article Info***
***Volume 82***
***Page Number: 15832 - 15838***
***Publication Issue:***
***January-February 2020***

***Article History***
***Article Received****: 18 May 2019*
***Revised****: 14 July 2019*
***Accepted****: 22 December 2019*
***Publication****: 28 February 2020*

***Abstract:***
Wireless body area network is an emerging technology used in our daily life to monitor the routine activities related to our health on daily basis like location, body posture, movements, temperature, etc by using sensors that collect information and through the internet like personal server information sent to the hospital only authorized doctor can view the original message. Providing security and privacy to the location attribute is important. In the modern era, various applications provide access to our location services. In the case of emergency, the current location can only share with the hospital staff so that they can easily find the current location of a patient to protect the location privacy, we examine different methods purposed by different inquires about the location privacy

***Keywords:*** *WBAN, Privacy, Security, Location*

## INTRODUCTION

Wireless body area network is a technology that accumulates the patient's physiological data from the various sensors and saves that data into aggregated node information and packet store into the hospital's database across the network. According to the Health Insurance Portability and Accountability Act (HIPAA) 1996. HIPAA is a collection of various privacy rules related to the patient's health. The data must be confidential. Data should not be leaked or stored securely in the database. All the physiological collected data send to the aggregate node and that encrypted data store into the hospital's database and only authorized person can decrypt the data and see the original message Fig: 1.Fresh and updated data stored in the database. Wireless body area networks are of mainly two types implantable and wearable. Wearable technology like smart jewelry such as rings, bands, etc. that connect with the smartphone and save all the data into the phone application.

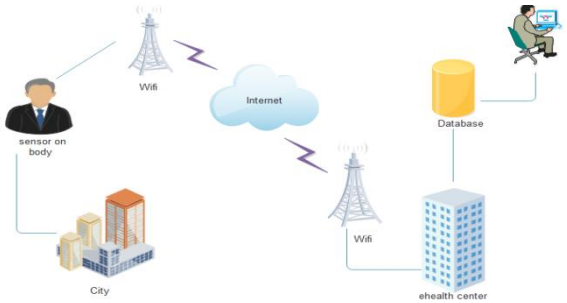


**Fig 1: WBAN Architecture**

Another example of wearable technology is a smartwatch that consists of sensors in it like in Fig: 3. Those sensors collect data like body temperature, blood pressure, sugar level, body movement, etc. While implantable sensors are placed under the skin to find the problems inside the body through various sensors that placed in different parts of the body. With the help of implantable sensors data, it is easy to diagnose the problem and doctors prescribe the treatment to the patient. Various technologies are used in WBAN like Fig: 3, which show the Zigbee, Bluetooth, WiFi, cell systems, etc. In WBANSecurity and privacy is the main concern. One of the significant security issues in Wireless Body Area Networks (WBANs) is Location privacy. The hostile party monitors the place and communication time between the sink node to the database. To make things even more regrettable, the

January-February 2020
ISSN: 0193-4120 Page No. 15832 - 15838

assailant doesn't need to be physically near the devices, can utilize a device with more power to communicate. It breaks the security of the user, it is up to the third party the information is revealed or not. To protect the location information of users apply the strong encryption technique.

**WBAN Three-Tier Architecture**

WBANs architecture Fig: 3, separated into three different tiers as follows:

***WBAN Tier-1***:- Tier-1 is used for data propagation. It is also called an intra-ban communication network. This communication is done between the sensors and the sink node of the WBAN. In these wearable sensors placed on the patient's body, they can monitor the temperature, glucose, ECG etc.

***WBAN Tier-2***:- Tier-2 is used for transmission of data. It is an inter-ban communication network. This communication takes place among sink node and personal server or personal digital assistant. It transmits the information through local servers to the base station or in the hospital database.

***WBAN Tier-3***:-Tier-3 is used for data storage and access. It is also called the beyond-ban communication network. This information is finally stored in a database and shows the information or data to the health care professionals.

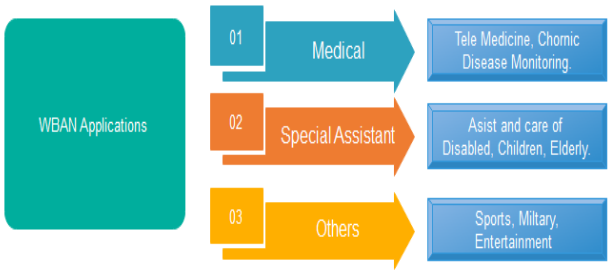


**Fig 2: Applications of WBAN**

WBAN applications Fig: 2 contain information related to the medical field like telemedicine, chronic disease, patient monitoring. In special assistant assist and care of disabled, children, and others in a sports field, military, entertainment. Wearable devices store all the personal information like user id and password, health-related data.

**SecurityChallenges in WBAN**

Data Encryption: - In data encryption plain text converted into the ciphertext means original message converted into some unreadable message. Humans cannot understand the message without decrypting it. The master node sent the information into the database. That information is in the encrypted format and the data remainsconfidential.

Two types of Encryption Techniques.

1. Symmetric key encryption: - In this encryption technique both the sender and receiver are having the same type of keys. If a patient is requested to store the data into the server. The sender sends the message in the encrypted format and the doctor who received that information is using the same key to decrypt the original message. It is called symmetric key encryption.

2. Public key encryption: - In this encryption technique pair of keys are used one is a secret key another is the public key. Users encrypt the data with the private key and create a digital signature on the message to make Information more secure.If anyone is used that same public key combine with the message, public key verify the digital signature weather the signature was valid or not, The receiver decrypts the message with the private key and verifies the digital signature. It is also known as asymmetric key encryption.

Data Integrity: - Data integrity means to ensure that the data sent through the network is not modified or it is secure. Only an authorized person can access the original message. Like patients send their medical information to the doctor and an only authorized doctor can access the original message. To maintain integrity the information is only sent to the authorized website. The encrypted form of data can be sent through the network and original data is stored into the database.

Authentication: - It a procedure to identify the user entity. Users can identify with the unique identification number and password. In this only authorized persons can access the privileges. Patient can give the correct identification number and that identity match with the database then the patient can edit their profile data related to the blood pressure, heart rate, etc daily and a doctor is having its identification number to view the medical records of the patient and prescribe the treatment according to the patient's information.

January-February 2020
ISSN: 0193-4120 Page No. 15832 - 15838

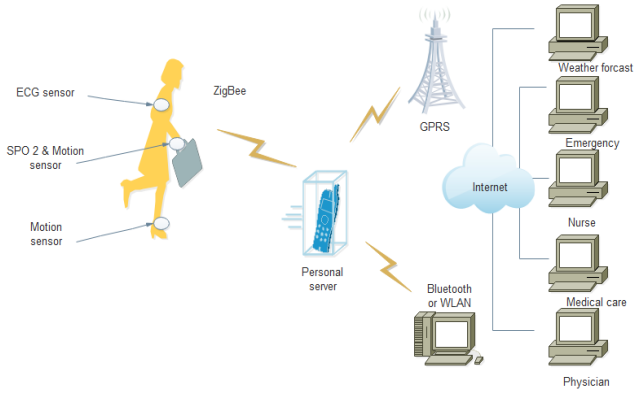


**Fig 3: Communication in WBAN**

Data Confidentiality: - To protect our information from third-party access. The master node sends the data into the database data should not be modified. To make data confidential use the encryption technique. Only the person who is authorized can access personal information. For example, only patients and doctors know about the problem. Share the information between both the parties. If someone knows the sensitive data it may get harmful results. Confidentiality can be obtained with encryption of data and sharing the keys between the sender and receiver.

Scalability: - It means to add several users in the system and properly handle them. Patients and doctors can easily communicate with each other to give equal rights to every user.Some basic requirements have to be fulfilled like authentication, confidentiality, integrity.Several users can connect with each other.Hospital databases more required a database to perform various other tasks like an emergency list of patients and old age people who suffered from the same disease.The workload is divided and we can easily identify the problem.Maintain the records are much easier. Make a type of system that can be easily managed even if there is any kind of update is required.

Data Authenticity: - It means that the quality of data is good and it is the original form of data.Authentic data represent a real-world scenario. If data processing has done the sense of data is not modify.The data cleaning process can be followed. If errors are found throughout the cleaning process then fix the error.New variables are constructed and applied to the cleaning process. Coordinator node and data node is having different rights to store the data.

Flexibility: - The term flexibility refers to easily adapt the changes according to the nature of the network resources, design requirements, topology, etc. If any other type of network connection with our network it can easily adapt the design requirements of our network with this communication is effectively done between the nodes. The WBAN network should be flexible so that nodes can easily communicate with the sink node and communication should not be interrupted.

Data Freshness: - Data freshness is an essential aspect that supports the integrity, confidentiality of data. If data packets sent over the communication channel check they are in the proper format or not. Freshness format divided into two types' strong freshness and weak freshness. In the strong, we know that packets sent properly. In the weak freshness, check the delay of packets and record is stored in the database. Always store the fresh and up to date information in the database.

**Location Privacy in WBAN**

Location privacy defined as information is sending through the network may have not been leaked or our real-time location should not be shown to anyone. The main known of this act is in England's 1361 Justices of the peace act constitutes arrest a stalker and eavesdroppers. In the US right to privacy and in 1890's US Supreme Court Justice Louis Brandeis "the right to be alone". 1984 Universal Declaration of Human Rights announces thateveryone has its privacy rights at home, family, and society.Under the act of the Information Technology Act, 2000 and (Indian) Contract Act, 1872 for data protection to maintain information keeps saving.Data privacy is to keep our information away from realizing one's present and past location. For example, if the HIV patient is visited in a hospital sat daily basis the location service is on the attacker know. Never reveal their visits in any location-aware application at their workplace, insurance companies, and bank. If a person withdraws their cash from bank another person with harmful intentions is relating an individual's data with the user's identification data may steal your money. At the time online transaction to keep your location services off it may be possible that someone tried to access your request.

**Location Privacy Model in WBAN**

In Fig: 4, the master node sends all the collected data to the hospital's database and data is an encrypted format.The person who is having the secret key is decrypting the original message. When data is sent from the master node to database location privacy comes in the picture. The hostile party attacks the encrypted data and

January-February 2020
ISSN: 0193-4120 Page No. 15832 - 15838

the attacker knows the patient's current location. Use that location information in a harmful manner they revealed that information to the bank, to the insurance company, and others as well. So it is important to protect our location information from third-party access.

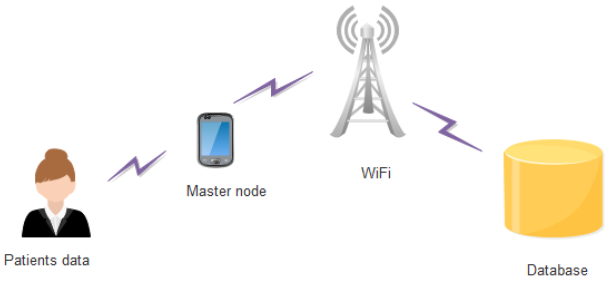


**Fig 4: Location Privacy Model in WBAN**

The patientsends the request with their medical record to store into the hospital's database and the doctor response to the request. This communication is unidirectional. The patients have to look at the location-aware applications and only show the location to the hospital staff so that they can send the ambulance as soon as possible in only authorized doctor can decrypt the data.

**Possible Location Privacy Attacks in WBAN**

There are various types of privacy attacks discussed as follows:

1. Single point attack: - In this attacker analyses the one query and to say that update the more information about the position or know the identity of the user. It is further divided into two parts:-

(1)A location homogeneity attack: - It used against the K-anonymity approach. The attacker identifies the position of the clusters and the location of the users.

(2)A location distribution attack:-In this users are in different clusters. Members of clusters covered under the densely and sparsely populated area.

2. Context linking attack: - In this attacker knowledge about the personal context information about the user and it's background. Further divided into two parts:-

(1) The probability distribution attack: - In this attacker find the probability of the distribution function and the location of the user.

(2)Map matching:-Removing all the irrelevant areas and restrict obfuscation area to a certain location.

3. Multiple position attack: -The attacker tracks the multiple location updates to breach security and privacy.

(1) Identity matching:-The attacker finds the links and Identify the co relational attributes.

(2) A shrink region attack: - Can find the Identity and location of the user. The attacker monitors all the activities.

(3) Region intersection attack: - Used to opposing location find the user's privacy and sensitive data. And obfuscation area decreases the user's privacy.

(4) Location tracking attack:-Trace the actual location of the user. This attack is against the randomly changing the locations without using the mix zones

(5) Maximum movement boundary attack: - Calculate the movement of the area, where the user is moving two locations and update the quarries.

4. Combination of multiple position and context linking attack: - In this attacker combine the two or more attacks. And maximum movement boundary attack to know the location of the user.

5. Compromised TTP: - In this attacker access the data to be stored clients data.

**Location Privacy Protection System in WBAN**

1. Centralized: - In the Fig: 5, a centralized network, architecture handles all the data. All data nodes connect with the central server. And save all information into the server. All nodes keep the information up to date and control all the network activities. Easy to collect and track the information. In the centralized system workload at the same system. Slower the speed of data transmission or response time also. Lack of bandwidth in this type of network.

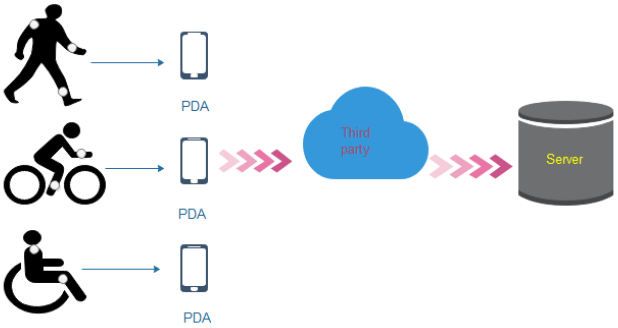


**Fig 5: Centralized approach**

2. Decentralized: - In the Fig: 6, decentralized system architecture, the workload is distinctamong the various users. Users may create a peer-to-peer network connection. This is a type of network with no single point failure. Easy to connect the nodes with other nodes for the transmission process. It provides more privacy than centralized architecture. Easily detection on if there is any problem.

January-February 2020
ISSN: 0193-4120 Page No. 15832 - 15838

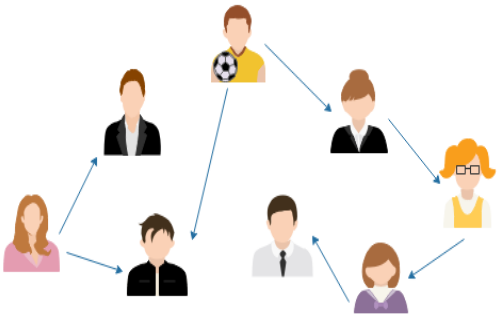

**Fig 6: Decentralized approach**

**WBAN Privacy Techniques**

**Privacy-preserving classification: -** In this [4] Privacy-preserving classification scheme (PPC). Classifying the patients' encrypted data at the WBAN gateway. WBAN gateway classifies all the data from the sender's side and pass the packets according to their priorities. In priority heap, all the packets are stored or transmitted for further processes. WBAN considered as semi-honest which means the WBAN gateway would strictly execute the protocol to guarantee the correctness of the medical packets relay task, WBAN gateway cannot recover the user's data. The threshold should not be recovered by the users and WBAN gateway. This PPC scheme is efficient in computational cost and communication overhead.

**Elliptical curve cryptography:** -This author [1] proposed Elliptical curve cryptography is used to implement the generation of the key. And Diffie-Hellman is applied for data privacy to protect our data from unauthorized access. In this role-based access is used two types of users one is patient and another is a doctor. Whenever patient signup into the device show his/her details and their thumbprint also detected. The Diffie-hellman algorithm is used for encryption and decryption processes. Patients can store new records related to their health. Whenever a doctor logs into the device view the encrypted data and the doctor will access that data encryption is performed using the ECC algorithm. After this doctor able to see the health status.

This paper shows [10] securing data transmission granting the confidentiality, authentication privacy and integrity elliptical curve cryptography technique is used this is a smaller, faster and more efficient cryptography algorithm RSA, DSA and DH. Many use the elliptic curve digital signature algorithm. Real-time access to users. ECC uses a good level of security and confidentiality is also a faster response. The author discusses the [9]Key management cryptography is used Elliptic curve cryptography and biometric is analyzed. Biometric is more useful than the cryptographic key distribution. Real-time monitoring of the health of the patient.

**Multiple biometrics-based schemes: -** The paper[11] proposed the multiple biometrics to generate a random key for inter sensor communication. Sensors attached to the patient's that data store in a personal server, this is two modes of framework is used Indoor and Outdoor. Inter body communication works that route the patient data to the remote base station through the personal server. Within the range of the first patient and if data is directed with the cloud then it stores in the EMR. That system works like a hospital Database. Multiple biometrics-based schemes increase the length and get a more random key and security key. Generated key verify the received message authentication code (MAC). Multiple biometrics security solutions for ubiquitous mobile healthcare.

**Block chain and DVSSA Scheme: -** This paper propose a block chain to solve the storage and unauthorized content from the third party use the sequential aggregate signature scheme with (DVSSA) Designed vertifier. Block chain to store the WBAN user's information which protect the data from being tampered and in DVSSA data can only view by the administrator. In the block chain no centralised server. It is use the peer to peer connection. Every node is engaged with other node. New node finds the nodes to communicate with each other. Less chances to failed. In block chain each node is connect and share the information. Invalid transaction is discarded. In the block chain attack on the information is harder. In DVSSA size of the signature written into the block chain equal to the size of a single person's signature. Sequential aggregation save the people's signature and save the storage space. Private data is stored into the different blocks in the form of link list in the cloud. The data stored in the cloud. Store all the data stored in the DVSSA and send to the block chain. If the patient 1 data is generated store that data into the data1 and with this corresponding private key is generated Sk1 and so on. At the end signed the manager's public key attribute to get the final signature and write it into the block chain. DVSSA scheme makes the bilinear map.

*January-February 2020*
*ISSN: 0193-4120 Page No. 15832 - 15838*

**Secure mutual batch authentication: -** In this paper author explain the remote batch authentication scheme discover the identity of application provider. Basically it is a combinationof elliptic curve cryptography and Bilinear paring scheme. Purpose solution reduces the computational cost and communication. It gives the efficient data aggregation and mutual batch authentication for finite resources in WBAN. Elliptic curve cryptography cannot give the genuine anonymous data, while users attribute could be use to track the corresponding clients. Improved cryptosystem based on a user's Identity was presented to securely authenticate different entities using bilinear paring. This purposed solution is suitable for the scenario of single authentication model with a less number of nodes. Elliptic curve cryptography is a key encryption scheme is based on ECC with generate faster, smaller and efficient cryptosystem keys.164 bit key is used with low computational cost and device battery usage. Short length of security key is used and the strong assumption to solve the ECC. In the bilinear paring two cyclic group E1(additive) and E2 (multiplication) of order P. Let g is a generator of E1 and e is a bilinear mapping. In this design a strong mutual batch certificate less authentication scheme between the controller and application provider. This scheme provide guarantee that no one can change any type of information.This scheme provides the Homomorphic encryption reduce the devices in the WBAN environment.

**Hybrid solution**: - This paper purpose the [13] hybrid solution HYB. Location privacy provides the mobile users it mainly pre-processes the location of the user's-anonymity once the congregation is formed, the centroid is calculated in such a way participating user's location is not revealed. It hides the position of the end-user. A K-1 user forwards the anonymizer query to the LBS provider. Difficult to identify the right user from a set.HYB solution works well for the more personalized queries for the user's specific needs. The decentralized approach is peer to peer and randomly selects the node to carry the communication between queries and the LBS server.Congregation model that K-1 users to create a group and compute the aggregate with knowing the actual location. The agent sends the meantime to the nearby nodes and sends the acknowledgment. In Homomorphic encryption, it uses the addition and multiplication because in the cloud database only decrypt data send but through this Homomorphic encryption we apply some of the rules of addition and multiplication and decrypt the data and send to the database.

**CAST model**:-This paper shows [12] the decentralized or third trusted party free architecture. The purpose of peer to peer communication model scheme that works on low latency and works efficiently.In the LBS it needs the exact location coordinate information for providing the location services to the user and it to leak your data for a particular motive and also that link with some other purpose like advertising.In this CAST model address, users carried the handheld devices like mobile, PDA's these were having already positioning capabilities. The CAST model is a decentralized approach to the set of having the same type of interests. For example, people driving in the same direction it is obvious that they might be reached at the same destination. This algorithm provides low latency privacy preserved location.

**Table of comparison**

| Technique | Advantages | Limitations |
|---|---|---|
| Privacy preserving classification | Communication cost is low. Efficient in the computational cost. WBAN gateway calculates the priority of each medical packet. | |
| Elliptic curve cryptography | Key size is small than RSA. | ECC algorithm is more complex and more difficult to implement than RSA, which increases the likelihood of implementation errors, thereby reducing the security of the algorithm. |
| Multiple biometrics based scheme | | |
| Block chain and DVSSA | Peer-to-peer communication | If the manager's signature attribute |

*January-February 2020*
*ISSN: 0193-4120 Page No. 15832 - 15838*

| | | |
|---|---|---|
| scheme | in the block chain. DVSSA to store the data in the form of link list in the cloud. | is lost then we cannot store the data into the block chain. |
| Secure mutual batch authentication | It reduces the communication and computational cost and provides the high efficiency. | It cannot predict the misbehaving nodes and avoid the collision attack due to the lack of trust. |

**Conclusion**

WBAN data is transfer between patient sensor nodes and save into the database. But our main focus on location privacy. Using various types of privacy techniques discussed by the inquire to secure the current location of a patient two types of approaches used in location privacy protection system centralized and decentralized. Analysed various techniques that protect our location privacy with different schemes.

## References

[1]. Er. Sandeep Rana, Sandeep Singh Kang "*Implementation of Biological Key Based Security Technique in Wireless Body Area Networks*", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-8, June 2019.

[2]. Laura Victoria Morales, David Delgado-Ruiz, and Sandra Julieta Rueda "*Comprehensive Security for Body Area Networks: A Survey*", International Journal of Network Security, Vol.21, No.2, PP.342-354, Mar. 2019.

[3]. SantanuChatterjee, Ashok KumarDas, Jamuna KantaSing"*A novel and efficient user accsess control scheme for wireless body area sensor networks*", https://doi.org/10.1016/j.jksuci.2013.10.007.

[4]. GuomingWang ,Rongxing Lu , (Senior Member, Ieee), And Yong Liang Guan." *Achieve Privacy-Preserving Priority Classification on Patient Health Data in Remote eHealthcare System*" Digital Object Identifier 10.1109/ACCESS.2019.2891775 2019.

[5]. WenchengSun, ZhipingCai ,YangyangLi, FangLiu, ShengqunFang, andGuoyanWang "*Security and Privacy in the Medical Internet of Things: A Review*" Security and Communication Networks Volume 2018, Article ID 5978636, 9 pages https://doi.org/10.1155/2018/5978636 .

[6]. E. Ahn, J. Kim, L. Bi, A. Kumar, C. Li, M. Fulham and D. D. Feng, "*Saliency-based lesion segmentation via background detection in dermoscopic images*", *IEEE journal of biomedical and health informatics*, vol. 21, no. 6, pp. 1685-1693, 2017.

[7]. Puning Zhang, Jie Ma, "*Channel Characteristic Aware Privacy Protection Mechanism in WBAN*", doi:10.3390/s18082403, 2018.

[8]. KoushikKarmakar, SohailSaif, Suparna Biswas "WBAN Security: study and implementation of a biological key based framework",2018.

[9]. M *Raj Kumar Naik, P.Samundiswary "Wireless* Body Area Network Security issues- Survey",2016 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT) , 2016.

[10]. Boukri Khalil, NajibNaja "*A Framework for Security Analytics of WBAN/WLAN Healthcare Network*", 2018.

[11]. FarrukhAslamKhana, Aftab Alia, HaiderAbbasb, Nur Al HasanHaldarc, "*A cloud-based healthcare framework for security and patients' data privacy using wireless body area networks*,"ComSense-2014.

[12]. Ruchika Gupta and UdaiPratap Rao "Achieving Location Privacy through CAST in Location Based Services"2017.

[13]. RuchikaGuptaand,UdaiPratapRao"A Hybrid Location Privacy Solution for Mobile LBS"2017.

[14]. Oladayo O. Olakanmi, Lightweight Security and Privacy Scheme for Wireless Body Area Network in E-Health System 2017.