THINK INDIA Journal

ISSN:0971-1260
Vol-22-Issue-16-August-2019

Recent Trends In Security and Privacy and Applications of Wireless Sensor Networks

Ashutosh Sharma
School of Electroics and Electrical Engineering
Lovely Professional University
Phagwara, Punjab, India
Sharmaashutosh1326@gmail.com

Pawandeep Kaur
School of Electroics and Electrical Engineering
Lovely Professional University
Phagwara, Punjab, India
pawandeep.kaur@lpu.co.in

Naveneet Kaur
School of Electroics and Electrical Engineering
Lovely Professional University
Phagwara, Punjab, India
navneet.19329@lpu.co.in

Abstract—Due to abundant advancement in wireless sensor networks technology (WSNs) make it possible to be used widely in monitoring the different events taking place in our daily life. The hot events such as military applications, healthcare management, ecology, environmental studies, forest fire detection etc. takes place at the top of the WSN applications. All the collected data from different areas requires high attentions for the security. There are different issues and challenges in the WSN such as the energy efficiency, placement of sensor node, storage capacity and operational complexity and so on. The major security issue exists here because communication occurs with the wireless method where security breach is a loophole option for the intruder. To strengthen the security issues there are certain schemes which allow the secured communication at each step. In this paper, certain security issues and challenges are discussed for the WSN communication. In the last, different security and privacy mechanisms are discussed which used in healthcare data management.

Keywords—wireless sensor networks (WSNs),security attacks, cryptography, security schemes, healthcare data security

I. INTRODUCTION

The wireless sensor networks (WSNs) is the network which has number of different sensor nodes used for sensing and transmitting the data. The reason behind the popularity of WSN in different applications is because of the certain features viz. small in size, low-cost, minimum energy consumption, minimum complexity [1]. The advancement in wireless communication enables us to use the wireless sensor networks (WSNs) in different areas of applications such as military surveillance, environment surveillance, healthcare surveillance [2], Transport traffic surveillance [3], agriculture crop surveillance, manufacturing, environment changes etc. The applications of tiny sensors can be made applicable from small scale to large scale sensor area which consists of different units of sensing, data aggregation and processing and communication from remote locations to base locations. The nodes which take part in the applications requested to be secured, safe from the data breach and malicious entry [4].

The use of WSN has been increased with inclined rate because of its features such as self-healing, dynamic topology due to node failure, standby in bad environment, scalable, self-organized etc. But due

ISSN:0971-1260
Vol-22-Issue-16-August-2019

to wireless nature of sensors, sometime it's hard to manage where security is a prime aspect as the probability of attacks is more [5]. In this paper we are addressing different security issues and challenges occurred while competing with WSNs.

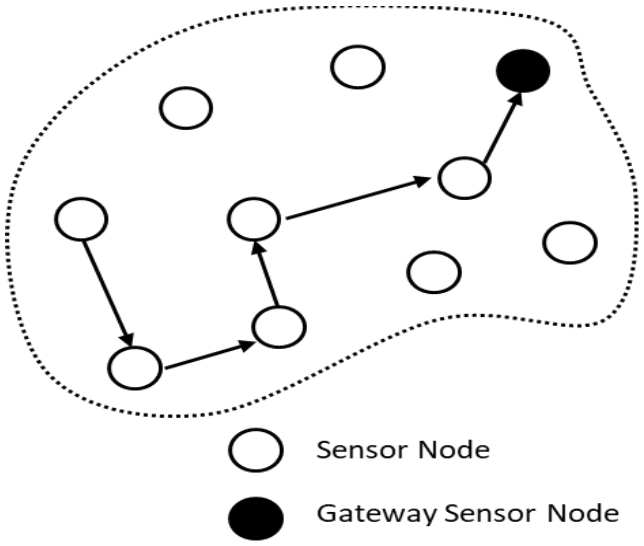

Fig 1 Wireless Sensor Network

Before jumping to security issues it's good to understand the design of WSN and challenges faced during WSN design. The WSNs has limited resources such as power at nodes, storage possibility may leads to unattempt data or missing data. The number of uncertainties such as natural disasters, manmade disasters etc. associated with nodes leads to unreliable environment for sensor nodes. Resources wastage due to multi-hope communication is also a challenge in WSN [6].

A. Outcomes

The certain outcomes of exhaustive literature is seen in broad sense and listed as below:

- Applications requirements for security
- Security issues in wireless sensor networks (WSNs)
- Security arracks occurred in WSNs
- Security schemes for WSNs
- Healthcare data privacy and security – A study

B. Organization

The rest of the paper is organised as follows: section II explain the necessity of security in WSNs. Section III is used to explain the different attacks in WSNs. Different security schemes are given in the section IV. A case study on healthcare data security is illustrated in section V. Finally, conclusion is drawn in the section VI.

II. NEED OF SECURITY IN WSNS

The WSN research area is fast growing and lot of applications are embedded with it such as automatic door locker, smart home etc. However, due to diversified research area the chances of getting vulnerable toward treats. These threats are the reason for the poor the performance or temper the information. These threats are sometimes hard issue for the mission-critical application such as critical-healthcare, location of soldiers in battlefield etc.

The requirement of security for the WSNs is known with certain points which are shown as below [7]:

ISSN:0971-1260
Vol-22-Issue-16-August-2019

A. Critical Data Integrity

In the present era of communication, critical services like healthcare reports are transmitted to remote laboratories. These types of reports data can't be shared with anyone without permission.

B. Unauthorized Data Access

The advancement in healthcare test over remote laboratories such as reports of HIV test are required to be safe without sharing the personal information of the patients.

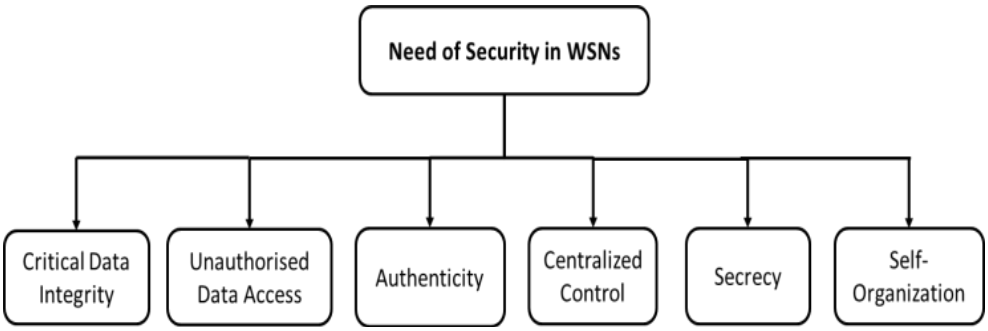

Fig. 2 Classification of necessity of security in WSN

C. Authenticity

The authentication to access the data centres, weather data is originated from authentic person or not. Authentication provides the detail of spoofing of data.

D. Centralized Control

All nodes in the network are connected together with each other from the base station and if base station got crashed services can be down of information can be leaked so its necessary to provide the security to the base station.

E. Secrecy

In WSNs it can be a case that intruder gives the number of copies to the network and get a loophole so therefore key management system needs to be placed that once a message sent or received it can't be read\write or changed by nodes itself.

F. Self-Organization

The major concern with the security requirements is that nodes are self-organized and if a node removed or added it can't be knows weather node is authentic or note.

III. ATTACKS IN WSNS

The attention for the attacks has been made because of the implications caused in the WSN such as slow performance of network, virus, multiple copies of traffic i.e. flooding and many more. In literature it has been shown that there are number of different attacks associated with the WSNs and given as follows[8, 9]:

A. Active Attacks

The major category of the attacks comes under this type of attacks. In these types of attacks intruder\attacker tries to take all the network control on its hands. The lists of various active attacks are: (i) Black hole (ii) Flooding (iii) Jamming (iv) Spoofing (v) Denial of Services (DoS) (vi) Traffic analysis and (vii) Hello floods.

DoS attack is the attack to prevent the users to use the computer resources. These attacks motives can may be varied from attack to attack such that prevent the working of site, target to high profile servers banking, payment gateways etc.

ISSN:0971-1260
Vol-22-Issue-16-August-2019

Hello floods attack is a self-natural attack and can't be predict with a high rate because generally in a network this message is occurs but if a stream of these mesas age came then it can be a hello flood. This attack keeps busy the server with the hello message and intercept takes place with the side of these attacks.

B. Passive Attacks

In these types of attacks attacker tried to access the information shared over the network without any knowledge of user. The types of passive attacks are traffic analysis, eavesdropping, traffic monitoring etc.

The traffic analysis attack is used to intercept the message and analysis the pattern of communication continuously to extract the information.

The eavesdropping attack is the attack which occurs with any knowledge of the attack. In this attack private conversation are intercepted mostly.

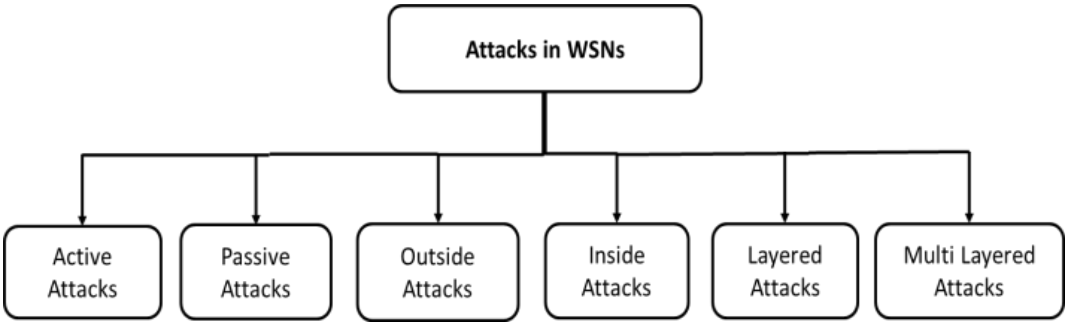

Fig 3 Different attacks in WSN

C. Outside Attacks

Eavesdropping is provide a major content for outside attacks which insert number of bugs and packets which waste the network resources. Also DoS is a major component of outside attacks.

D. Inside Attacks

This types of attacks acts as a silent killer such as if we discuss the grayhole attack where faulty nodes pretend to be working nodes and hence very difficult to handle this type of attacks. These controlled nodes are known as compromised nodes.

E. Layered Attacks

In computer communication there are number of layers and each layer has its own functioning. These attacks are categorised in different bullets given below:

- Physical layer attacks: This layer is generally used to broadcast the message and the attack used here to jam the message from broadcasting. Also, this layer is close to the attacker and can be gain the access to control over the broadcasting of a message.
- Link layer attacks: This layer basically provide the one hop connectivity to the other nodes in the network. The main component is the medium access control (MAC) used to coordinate the transmission of nodes, but this protocol is not suitable for connecting radio links. The attacks in this layer can used to degrade the life time of nodes called as Denial of Sleep. To increase the energy consumption at nodes is also in the category of the attacks.
- Network and routing attacks: The attacks on this layer are server and studied widely by the researchers. By studying and attacking the routing protocol, one can gain easily access to its resources. The routing protocols work in this layer and therefore routing flow, traffic monitoring, path between sources and destination can be controlled if this layer got attacked.
- Transport layer attacks: The main protocol in this layer is transmission control protocol/user datagram protocol (TCP/UDP). The TCP used here to provide the end-to-end data transmission

ISSN:0971-1260
Vol-22-Issue-16-August-2019

and fully relies on the three-way handshaking mode. The several types of requested are takes place here as SYN and ACK. The attackers control over these requests by hijacking the session of the request. By doing this the attacker can perform resource exhaustion, spoofing and DoS.

- Application layer attacks: The upper most layer is the application layer and several protocols are embedded with it such as TELNET, HTTP, ICMP, FTP, SMTP etc. At this layer these protocols are most vulnerable to the attacks because this layer is very close to the users and information. The attackers can perform the activity of data corruption and malicious attack on the useful data.

F. Multi Layered Attacks

These types of attacks are generally generated or launched from different layers such as man in the middle, DoS and impersonation attacks. The impersonation attacks are the attack which are performed by using the identity of other nodes such as MAC address, IP address. At this node the SYN flooding is also takes place.

The above list of the different attacks leads to develop and dictate the security schemes which are given in the next section.

IV. SECURITY SCHEMES IN WSNS

There are different security schemes in WSNs which are used to prevent the data to be breach. A wide literature shows its usefulness in WSNs, therefore the security schemes are categorized into two categories given as below[10]:

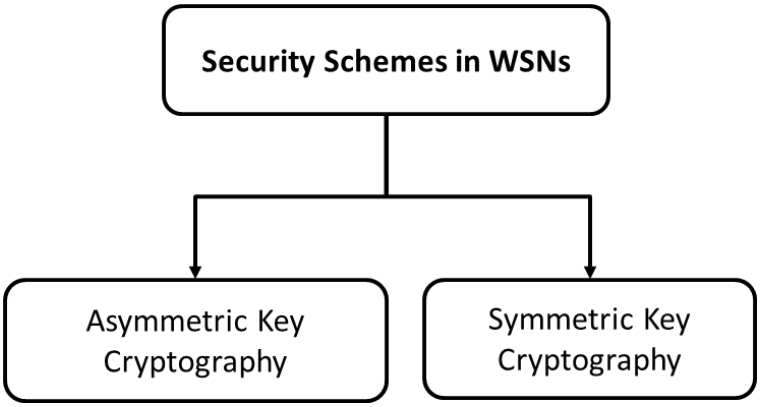

Fig 4 Basic security scheme in WSN

A. Asymmetric Key Cryptography

The asymmetric key cryptography is considered as very much complex to use in the WSNs. There are number of different schemes such as RSA, Diffie-Hellman and ECC which share the key protocol to provide the security. These schemes are computationally very complex and consume access storage in WSN sensor node. Some of the literature shows their usefulness when applied in terms of constraints.

In this scheme, keys are long enough which are paired together but these are not identical means asymmetric. One of the pair from the keys can share with everyone (Public) and other pair can be made private. The encryption of the message is made with the help of key and the opposite of the key is used to decrypt the message. The strength of encryption depends on mainly the key size and this strength can be increased with the help of doubling the key size. By doing this, the strength of encryption increased exponentially.

In literature, it is shown that if RSA and ECC are implemented on small devices without any modification in hardware, then these algorithms are also work excellently. Token type security also been used for security in WSNs by generating a token at base station. Further, this token is encrypted using

ISSN:0971-1260
Vol-22-Issue-16-August-2019

public key and each node when receive this token has to authenticate weather this token associated with their community or not.

The RSA is the most widely used asymmetrical algorithm which is embedded with the security protocol i.e. SSL/TLS. These protocols provide security over a computer networks. RSA provide the security from the computational difficulty of factoring large integers numbers which are the product of two large prime numbers. These large number are then multiplied to get the original number which is a quite difficult task. The size of RSA keys is either 1024 or 2048 bits long, however it has been thought by the researchers or experts that 1024 keys can be broken in the upcoming years. May be this is because of the high-speed computers, therefore government bodies and R&Ds are tried to use 2048 bits long keys.

Another scheme which uses the asymmetric keys is digital signature. This is the most popular scheme now a day to store the originality, secrecy of the document, transection of message and acknowledgement to the signing authority. The digital signature is created by the signing software by creating one way hash of the electronic data. A private key from the user has been used to encrypt the hash function and that hashing return a unique hashed data. The collective information of the encrypted message and the hashing algorithm forms as a digital signature. The beauty of this scheme is that if a single bit is changed then it results into a different hash value, therefore, this property enables others to validate the integrity of data with a public key to decrypt the data. If decrypted hash matches with the second computed data, then it proves that the data is not tempered. If two hashes are not matching, then there can be two cases either data is tempered or the key used to decrypt the message is private not a public key. The all two cases show that authentication is failed to recover the data. In many countries like USA, Canada, these keys have been given same rights as the signature.

B. Symmetric Key Security

This type of security is wasteful technique as keys and other secrete information loaded in sensor nodes before deployment and this information used to communicate with the other sensor nodes. The drawback of this type of security system is that if any breach in the security of node occurred or compromised then the whole network has to be compromised. This problem was a research gap and various researchers are working on this. The solution proposed by the researchers was that rather than global keys management, the keys are loaded in section or pair wise.

- The symmetric encryption scheme contains five main points as:
- The original message in terms of data which is given to the algorithm as an input.
- The encryption algorithm implementation which uses various substitution and permutation on the original message.
- Another input for this message is in terms of security keys and based on these keys output depends. These specific keys are responsible for different outputs.
- The message received after the encryption is known as cipher text which is the combination of message signal and key. This text is a random stream which is unintelligible.
- The last task in the program is the decryption algorithm which is same as reverse. The inputs for this steps are cipher text and keys which produce original message.

The main requirements of this encryption algorithm are:

- There is no need of hiding algorithm instead of algorithm the keys are requested to be keep secret.
- The keys have been given both sender and receiver secretly as if algorithm is public and can be known to everyone, therefore these keys are requested to keep secretly.

ISSN:0971-1260
Vol-22-Issue-16-August-2019

The main advantage of symmetric key encryption is that it has very less computational overhead as compared to asymmetrical encryption scheme.

The main examples of symmetric key encryption are given as: (i) DES (ii) DES3 (iii) AES (iv) TwoFish (v) BlowFish (vi) Idea and (vii) Chameleon

Data Encryption Standard (DES)

The 64-bit long cipher block is known as DES where 64-bit long block of original message i.e. plaintext goes in one end and cipher text block comes out from the other end. The reverse must be follow using same algorithm and keys to decrypt the cipher text. The length of the key is about 56 bit long and it can be of 64-bit long. The security of the scheme lies in the keys only.

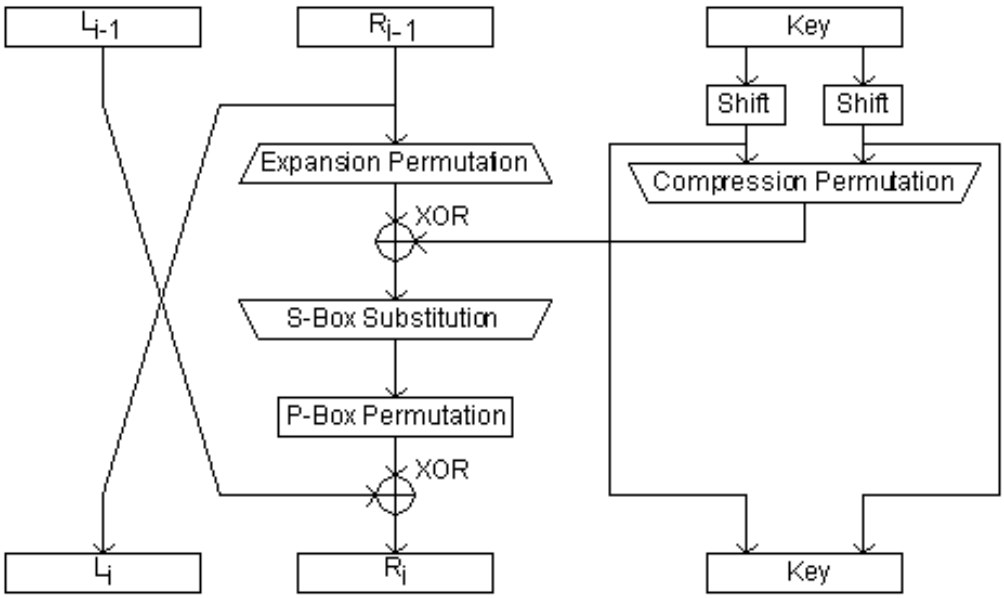

Fig. 5 The block diagram of working of DES

This encryption technique is nothing but the combination of two basic techniques (1) confusion and (ii) diffusion. The fundamental block of the DES is a single combination of these techniques on the original message based on the keys. This step is known as round and has 16 rounds. These rounds are applied same to the original text for 16 rounds. The applicability of the arithmetic and logical operation on the number of 64 bits at most. However, this scheme was good in 90s, but face problem when fast computer exists and evolved.

Advanced Encryption Standard (AES)

The AES algorithm is a symmetrical key encryption which replaced DES due to the certain limitations such as vision for data security over 30-40 years, worldwide access, easy implementation.

The working of AES algorithm can be portioned into three different rounds (i) Initial round (ii) main round and (iii) final round. The working of each phase is given as below:

- Initial Round: This round is very basic round and the main task is to add the round keys.
- Main Round: The main working of the paper lies in this round which contains sub bytes and shift rows. Another task is to mix the columns with each other and add the round keys from the intial round.
- Final Round: This round has the same steps but this last round contains different calculation method.

ISSN:0971-1260
Vol-22-Issue-16-August-2019

The main rounds are repeated for the nine times such that AES-128 uses 9 iterations of the main round. The encryption phase of AES can be broken into three phases: the initial round, the main rounds, and the final round. All the phases use the same sub-operations in different combinations as AES-128 uses 9 iterations of the main rounds, AES-192 uses 11 and AES-256 uses 13.

The difference between both schemes DES and AES has been given below for the more understanding:

Table 1 The difference between DES and AES symmetric key cryptography schemes

	DES	**AES**
Date	1976	1999
Block Size	64	128
Key Length	56	128, 192, 256
Number of rounds	16	9, 11, 13
Encryption primitives	Substitution, permutation	Substitution, shift, mixing, bit
Cryptographic primitives	Confusion, diffusion	Confusion, diffusion
Design	Open	Open
Design rationale	Closed	Open
Selection process	Secret	Secret, but accept open public comment
Source	IBM enhanced by NSA	Independent cryptographers

In the next section, the security attacks and schemes are explained related to application of healthcare data security.

V. HEALTHCARE DATA SECURITY AND PRIVACY – A STUDY

WSN founded healthcare system contains number of sensor nodes which communicate with each other through wireless communication. These sensor nodes measures numbers of different health parameters viz. temperature, heart rate, blood pressure. These sensor nodes are known as body sensors. The usefulness of these body sensor nodes is seen in the healthcare system where regular assistance is given to track and monitor the patient health individually. By getting the data from the body sensor nodes, doctor examines the patient state and advice to have some precautions. Thus, WSNs provided its applications in healthcare monitoring system for those who are differentially abled and the old age

ISSN:0971-1260
Vol-22-Issue-16-August-2019

patients who cannot visit doctors. However, in spite its useful applications in healthcare, there are certain challenges to use and adopt properly.

As the patient data sometime is very confidential and can't be shared with others because it can harness his privacy, therefore such type of implications restrict this technology as a part of our life. This type of technology are divided into several categories such as e-healthcare, m-healthcare, remote healthcare etc. which provide real time, non-real time monitoring, critical routing, offline and online monitoring [11].

These types of services are also useful for providing the useful data for research. The certain examples such as blood pressure measurement, heart rate, diabetes level are monitored at the remote locations by the experts. Although the data gathered from the patients is useful in research, but there is a chance of security and privacy threat for the patient. The secret data of the patient can be disclosed and the privacy of patient will be offended. The WSN used to get the medical data from the patient is known as wireless medical sensor network. The figure shows the placement of different body sensors for the medical data.

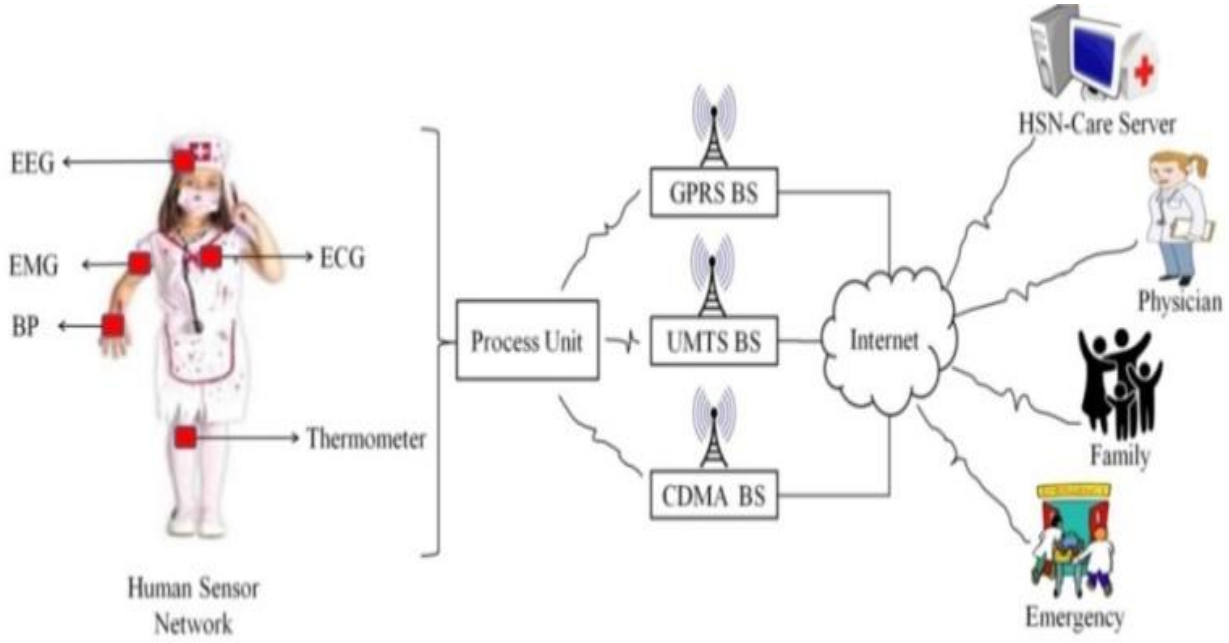

Fig 6 Architecture of WSN based healthcare system

The data is routed with certain protocols from remote location to the professionals for analyzing the health issues [12]. The medium used between remote location and professionals is the major part from where eavesdropping and other malicious activities on data can be performed which can be a threat for the patient. There are certain applications listed in the literature which are useful for the WSN such as, CodeBlue, Ubimon and Mobicare [13]. The WSN uses wireless communication, therefore, security and privacy issues.

The eavesdropping is very easy for the security break such as in this case hackers inject malicious message. The WSN is also having a great influence to the DOS or DDOS. Due to these security and privacy risk, certain algorithm and security methods are developed [14] i.e SHA-3, longwave encryption.

The privacy prevention [15] is studied by the researcher for the online banking. The information entered by the user goes to the service providers and at this stage attacker can easily embed his malicious or incorrect or previous data to the professionals. Therefore, to engage with this issue a security signature is generated. Another privacy prevention scheme is used as wireless equivalent privacy (WEP) is also used as the authentication between sender and receiver [16].

This scheme mostly used in multipath routing of data. Further, there are certain privacy prevention methods and schemes are listed in literature by researchers. The most aged privacy prevention scheme from World war – I is known as cryptography privacy prevention scheme but, there are some limitations with this scheme as it uses high computational overhead.

ISSN:0971-1260
Vol-22-Issue-16-August-2019

VI. CONCLUSION

The present paper used to understand the security and privacy threats associated with WSN. The different applications of WSN are discussed in this paper which shows the usefulness of WSN in various fields. The study of WSN is showing the vast applications in medical sciences but at the cost of risk and security threats. The medical data of critical patient can be misguided by hackers; therefore, the certain security and privacy schemes are used for the data so that it cannot be misused by the hackers. This paper shows that, each scheme is associated with certain advantage and limitations. The literature shows that numbers of researchers are associated with it for improvements. The study in this paper allows user to use the privacy and security scheme according to the requirements.

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Comp. networks*, vol. 38, pp. 393-422, 2002.

[2] H. Alemdar and C. Ersoy, "Wireless sensor networks for healthcare: A survey," *Comp. networks*, vol. 54, pp. 2688-2710, 2010.

[3] C. Wang, K. Sohraby, B. Li, M. Daneshmand, and Y. Hu, "A survey of transport protocols for wireless sensor networks," *IEEE network*, vol. 20, pp. 34-40, 2006.

[4] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Comm. of the ACM*, vol. 47, pp. 53-57, 2004.

[5] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *Ad hoc networks*, vol. 1, pp. 293-315, 2003.

[6] S. Mal-Sarkar, I. U. Sikder, C. Yu, and V. K. Konangi, "Uncertainty-aware wireless sensor networks," *Int. J. of Mobile Communications*, vol. 7, pp. 330-345, 2009.

[7] J. Lee, K. Kapitanova, and S. H. Son, "The price of security in wireless sensor networks," *Comp. Networks*, vol. 54, pp. 2967-2978, 2010.

[8] D. G. Padmavathi and M. Shanmugapriya, "A survey of attacks, security mechanisms and challenges in wireless sensor networks," *arXiv preprint arXiv:0909.0576*, 2009.

[9] H. Modares, R. Salleh, and A. Moravejosharieh, "Overview of security issues in wireless sensor networks," in *Computational Intelligence, Modelling and Simulation (CIMSiM), 2011 Third International Conference on*, 2011, pp. 308-311.

[10] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "SPINS: Security protocols for sensor networks," *Wire. networks*, vol. 8, pp. 521-534, 2002.

[11] A. Sharma and R. Kumar, "An optimal routing scheme for critical healthcare HTH services—an IOT perspective," in *Image Information Processing (ICIIP), 2017 Fourth International Conference on*, 2017, pp. 1-5.

[12] A. Sharma and R. Kumar, "Performance comparison and detailed study of AODV, DSDV, DSR, TORA and OLSR routing protocols in ad hoc networks," in *Parallel, Distributed and Grid Computing (PDGC), 2016 Fourth International Conference on*, 2016, pp. 732-736.

[13] J. M. Corchado, J. Bajo, D. I. Tapia, and A. Abraham, "Using heterogeneous wireless sensor networks in a telemonitoring system for healthcare," *IEEE trans. on information tech. in biomedicine*, vol. 14, pp. 234-240, 2010.

[14] X. Yi, A. Bouguettaya, D. Georgakopoulos, A. Song, and J. Willemson, "Privacy protection for wireless medical sensor data," *IEEE trans. on dependable and secure computing*, vol. 13, pp. 369-380, 2016.

[15] N. Li, N. Zhang, S. K. Das, and B. Thuraisingham, "Privacy preservation in wireless sensor networks: A state-of-the-art survey," *Ad Hoc Networks*, vol. 7, pp. 1501-1514, 2009.

[16] M. Rashed, M. H. Kabir, and S. E. Ullah, "WEP: An energy efficient protocol for cluster based heterogeneous wireless sensor network," *arXiv preprint arXiv:1207.3882*, 2012.