# COMPARISON OF SECURITY TECHNIQUES IN HEALTH MONITORING SYSTEM

Poornima.L[1], Vaijeyanthi.V[2], Sathya.D[3]
*1Department of Computer Science and Engineering,*
*Kumaraguru College of Technology, Coimbatore, Tamil Nadu, India*
*2Department of Computer Science and Engineering,*
*Kumaraguru College of Technology, Coimbatore, Tamil Nadu, India*
*3Assistant Professor II, Department of Computer Science and Engineering,*
*Kumaraguru College of Technology, Coimbatore, Tamil Nadu, India*

## ABSTRACT

*Wireless Medical Sensor Networks plays a key role in remote health monitoring system which is used to collect patient health parameters like body temperature, pressure, heart beat, glucose level etc. The health data will be send to the medical centers for diagnosis. The breach of health data may leads to a life threatening risk to the patients. So the collected data should be secured against various threats which would be the challenging task. Preserving integrity and privacy of data during transmission is really important. In this work, existing systems and its algorithm are compared for best performance. The work also shows the graphical comparison of encryption, decryption, and total throughput time.*

*Keywords: Wireless Medical Sensor Networks, Remote Health Monitoring System, integrity, privacy*

---

## I. INTRODUCTION:

One of the emerging technologies in Networks is Wireless Medical Sensor Networks (WMSN). It has numerous sensors to detect and monitor patient's body conditions. It has been widely used in Healthcare Monitoring System and also in other medical applications. In Healthcare Monitoring the sensors may be wearable or implanted based on the need. Due to advancement in wireless communications it is easy to monitor patient's body conditions. But in these networks there are adversaries who may intercept communication, delete or replace the information and send to the original receiver and eavesdrop node to cheat other person, sometimes data transmission is maliciously repeated or delayed etc[1]. To protect against those threats major things needed in WMSN is security. For that the data in the sensor has to be secured, so the data should be encrypted. The encrypted key should be shared among the sensors thus preventing adversarial to decrypt the data. Because adversarial do not have either encryption or decryption key [2].WMSN are used in emergencies where patient details should be retrieved against various disasters like hacking, human invasion and from other natural disasters. Unlike other applications Health Monitoring System should be authentic, available, integrity and confidential [3].

## II. RELATED WORK:

In [4], securing the data without affecting its accuracy is an important task. Unreliable communication channel and operation that are unattended make security defenses even harder against attacks. Those attacks may be either active or passive. AES and DES algorithm are implemented to secure sensed data in WSN.

In [5], to detect replay and jamming attacks in the Secure Network Motesec, efficient network layer security system provides security for both memory data and network message. For that a symmetric cryptography mechanism AES is used in the OCB mode and an access control Key Lock Matching (KLM) is used to prevent unauthorized access. Advantage of this system is that it consumes lower energy and achieves high security than the state-of-the-art methods.

In [6], stakeholder shares the data by three usecases and they are as follows, proof of ownership- the person is the originator of the data, data-tracking –data owner trace unauthorized sharing of data, content authentication- to prove that the data does not gets modified maliciously by other consumers. Thus robust watermarking technique is used to embed security information in the bio-signal data so that data gets unaffected. Bio-signals can be altered but watermarking cannot be spoofed, recovered or corrupted by malicious consumers. Thus data integrity is preserved by watermarking and the consumers can easily track the data.

In [7], to address the challenges for preserving privacy many techniques are used such as location privacy, data privacy, context privacy and network privacy and it is very challenging too. The challenges faced to preserve privacy are 1.Uncontrollable environment leads to physical attacks, 2.Sensor node resource constraints for store, process, transmits data, 3.Topological constraints.

In [8], for privacy preservation in WSNs when data has to be transferred to the public area many operations on cipher text homomorphic encryption scheme is used. Paillier algorithm can be used for preserving additive property of homomorphic encryption while RSA and ElGamal can be used for multiplicative property. Paillier algorithm is used in e-voting system and threshold scheme.

In [9] in order to maximize the network lifetime of wireless sensor networks High Energy First (HEF) algorithm a reference model for cluster head election which selects a node with the highest residual energy in every round is implemented. Further paillier homomorphism is used to provide end to end data security and confidentiality. Data has to sent by encrypting towards base station, sensors applies aggregation function on the data which is encrypted. Although base station receives minimum data, it provides security to the data even from the aggregator level.

## III. PROPOSED SYSTEM:

In Wireless Medical Sensor Networks the three existing systems [10], [11], [14] and its algorithm are compared for the best performance. The works are discussed below:

In [10], WMSN's senses body of the patient, transmit the data to the Patient Database System (PDS). PDS stores the patient data from the sensors and data can be queried by users like physician or medical researchers. There is a middleware between sensor and PDS which has the role of sending encrypted data to the distributed database. Then the data has to be securely transmitted from distributed database node to server node. For this secure transmission to occur, each data in the sensor is splitted into three parts such as $\alpha, \beta, \gamma$ such that their sum $\alpha + \beta + \gamma = \rho$. $\alpha$ is sent to the server s1, $\beta$ is sent to the server s2 and $\gamma$ is sent to the server s3 by using secure mechanism of paillier cryptosystem. Each server will create a database to store the data. If the user can get the intermediate encrypted data, the user cannot decrypt it without cooperation of all the three servers. As long as one data server of the distributed database is not compromised the privacy of the patient is still preserved.

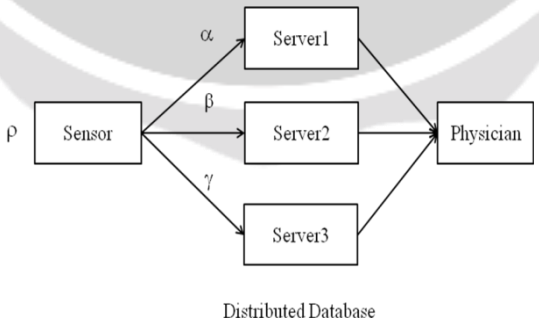


Fig. 1 Data collection

Paillier algorithm is used in this system and are explained below. It is an asymmetric algorithm for public key cryptography. It is an additive homomorphic system (i.e., encryption of message m1 and m2 gives the encryption sum of m1 and m2). Applications of this Paillier cryptosystem are E-cash which is to ensure that the e-coin is a valid one without disclosing person privacy and E-voting, method of voting digitally without disclosing voter's privacy.

A. *Paillier cryptosystem algorithm [10]*

*1) Key generation:*

1. Two large prime numbers '$p$' and '$q$' are chosen at random and independent of each other hence$\gcd(pq, (p-1)(q-1)) = 1$. This property is used if both primes are of equal length.
2. Compute $n = pq$and$\lambda = lcm(p-1, q-1)$.
3. Select random integer '$r$' where$g \in \mathbb{Z}^*_{n^2}$.
4. Check $n$divides the order of '$g$' by checking the existence of the modular multiplicative inverse:

$$\mu = \left(L\left(g^{\lambda} mod\ n^2\right)\right)^{-1} mod\ n,$$

where the function L is

$$L(u) = \frac{u-1}{n}.$$

Note that the notation $\frac{a}{b}$ does not denote the modular multiplication of $a$ times the modular multiplicative inverse of b but the quotient of a divided by **b**, i.e., the largest integer value $v \geq 0$ to satisfy the relation **a** $\geq vb$ .

- The public key for encryption is $(n, g)$.
- The private key for decryption is $(\lambda, \mu)$

If using p, q of equivalent length then $g = n+1, \lambda = \varphi(n)$ and $= \varphi(n)^{-1} mod\ n$ , where $\varphi(n) = (p-1)(q-1)$.

*2) Encryption*

1. Let $m$ be a message to be encrypted where m is in $\mathbb{Z}_n$ .
2. Select random number be $r$ where $r \epsilon \mathbb{Z}^*_n$.
3. Compute ciphertext as: $= g^m . r^n mod n^2$ .

*3) Decryption*

1. Let $c$ be the ciphertext to decrypt, where $c \epsilon \mathbb{Z}^*_{n^2}$
2. Compute the plaintext message as $m = L\left(c^{\lambda} mod n^2\right).\mu\ mod\ n$.

In [11], to secure WMSN in a novel and light weight system patient details has to be transmitted securely. In this Advanced Encryption Standard(AES), symmetric algorithm is used to provide security and SHA-1 algorithm is used to provide integrity. The system involves four phases, initialization phase is to setup the medical sensor network, joining phase is the phase before in which the user issues commands, regular use phase in which data securely gets transmitted to network server via controller, user command phase in this user commands and proxy signature are sent to the network server. If verification is successful network server responds to the command of the user.

User registers at the server to access patient details for that proxy-protected signature by warrant (PSW) is introduced. There are two users original signer and proxy signer. Signing power validates for some period of time only. Verification is done by verifiers to validate the proxy signatures with public key of original signer to the legally enter into the WMSN. Only registered user can access the data. Sensor sends the details in the format of (IDPANl , IDsj , {data}$k^r$j, h({data}$k^r$j_r, $k^r$j) to the server through the controller. If server has the decryption key then the server decrypt the data. Receiving the decrypted data server has to ensure that the correct data is sent by the correct user. For integrity of the data, server has to hash the data. If the currently received digest matches the sender then the message the receiver gets is a genuine unaltered one. If doesn't matches then the receiver drops the message. The algorithms used in this work are AES and SHA-1 they are described below.

The fig.2 represents the flow of information securely from sensor nodes to the server node thus providing integrity and confidentiality.

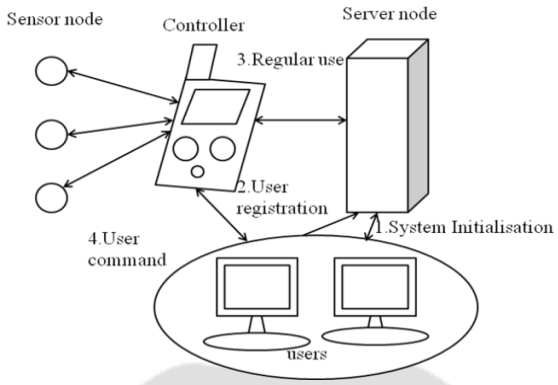


Fig .2 Flow of security information

*B. AES Algorithm[12][13]*

AES Algorithm is used in this system. It is a symmetric-key algorithm where the same key is used for both encryption and decryption. It has key size of 128,192 or 256 bits. It has block size of about 128 bits. It has 10, 12, 14 rounds based on key size. The algorithm is described below,

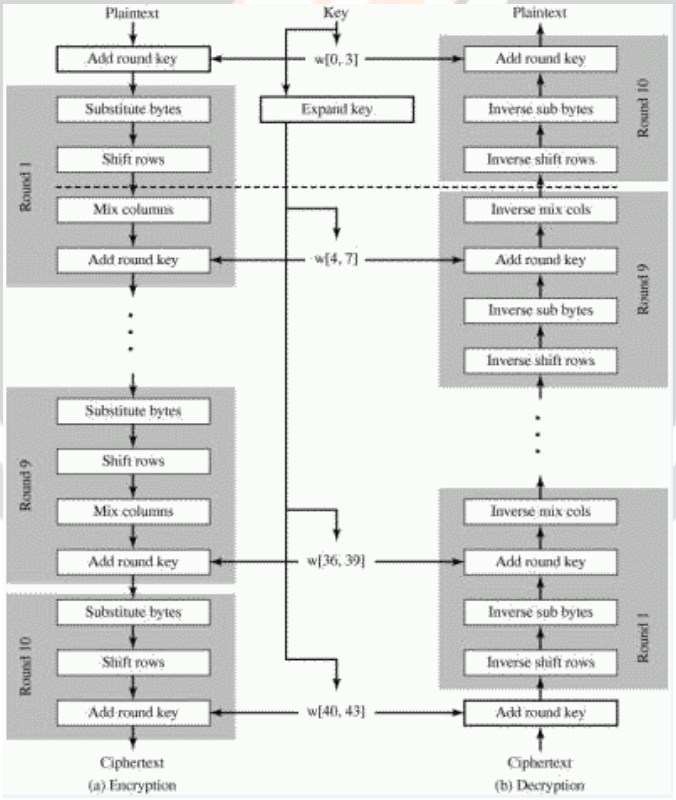


Fig. 3 Work flow of AES Algorithm

SHA-1 is used in this system. Original message gets padded so its length is congruent to 448 and modulo to 512. 64 bits are appended at the end of the padded message to indicate the length of the original message which is represented in bytes. It requires 80 processing functions. It requires 80 processing constants. It requires 5 word buffers with initial values. To process the message in 512-bit blocks, it undergoes loop of padded and appended message in blocks of 512 bit each. The output is the digest.

In [14], to secure messages the data communication protocol Ciphertext Policy Attribute based Encryption(CP-ABE) to perform communication between doctors and datasink to retrieve patient information or distribute

commands to the Body Area Networks(BAN). It uses access control structure to achieve role-based access control (RBAC). The sensor encrypts the body data and sends them to the data sink. The doctor contacts the data sink decrypts the session key and then retrieve the data using AES. CP-ABE provides asymmetric encryption to encrypt session key for establishing symmetric encryption .

C. *CP-ABE Algorithm[14]*

*1) System Initialization:*

1. Select a prime number $p$ and a generator $g$ of $G_0$, and a bilinear map $e: G_0 \times G_0 \rightarrow G_1$
2. Define a Lagrange coefficient $\Delta_{i,s}$ for and a set S of elements in Zp $\Delta_{i,s} = \pi_{j \epsilon s, j \neq i} \frac{x-j}{i-j}$
3. Choose two random exponents $\alpha, \beta \epsilon \mathbb{Z}_p$.
4. Select a hash function H:$\{0,1)^* \rightarrow G_0$. The function H is viewed as a random oracle.
5. Distributes the public parameters of the system given by $PK = G_0, g, h = g^\beta, e(g,g)^\alpha$
6. Computes the master key MSK is $(\beta, g^\alpha)$.

*2) Key Generation (MSK, S)*

Inputs: The master key MSK and the set of attributes S possessed by the user (a sensor or a data consumer) requesting a private key.

1. Select random number $r_{sn} \epsilon$ Zp, $K_{sign} = r_{sn}$, and calculate the verification key $K_{ver} = g^{r_{sn}}$.
2. The KGC chooses random numbers r; $r_j \epsilon \mathbb{Z}_p$ for each attribute $j \epsilon s$.
3. The secret key SK is computed by

$$SK = (D = g^{\frac{(\alpha+r)}{\beta}}, \forall j \epsilon s: D_j = g^r . H(j)^{r_j}, D_j' = g^{r_j}$$

4: Send SK and $r_{sn}$ to the owner of the attribute set S via a secure channel, and publish $K_{ver}$ for others.

*3) Encryption (PK, K, T)*

Inputs: User public parameter PK; session key K; the tree T rooted at node R specifying the access right of the key K.

1. Chooses a polynomial $q_x$ and sets its degree $d_x = k_x$-1 for each node x in the tree T.
2. Chooses a random $s \epsilon \mathbb{Z}_p$ and sets $q_R(0) = s$;
3. Chooses $d_R$ random points from $Z_p$ to completely define the polynomial $q_R$.
4. for any other node x in tree T do
5. Set $q_x(0) = q_{parent}(x)(index(x))$.
6. Selects $d_x$ random points from $Z_p$ to completely define $q_x$.
7. end for
8. Let Y be the set of leaf nodes in tree T. The ciphertext CK is constructed based on the access tree T as follows:

$$CK = (T, \tilde{C} = (g,g)^{\alpha s}, C = h^s, \forall\ y \epsilon Y:$$

$$C_y = q_y(0), C_y' = H(att(y))^{q_y(0)}.$$

9. Compute the signature by hashing the bitstring K, as h = H(K).
We output the signature $\sigma = h^{r_{sn}}$
10. Output the message:
CT = (CK, $\sigma$)

*4) Decryption (CT, SK)*

Inputs: A ciphertext CT = $(T, \tilde{C}, C, \forall\ y \epsilon Y: C_y, C_y')$; the secretkey SK; the set of possessed attributes S.

1. function (DecryptNode (CT, SK, x))
2. if x is a leaf node of tree T then
3. Let i = att(x)
4. if $i \epsilon S$ then

Return $\frac{e(D_i, C_x)}{e(D_i', C_x')} = e(g,g)^{rq_x(0)};$

5. else Return $\perp$.
6. end if
7. else
8. for each child node z of x do
9. $F_z$ = DecryptNode(CT; SK; z)
10. end for
11. Let $S_x$ be an arbitrary node of $k_x$-sized set of child nodes of x such that $F_z \neq \perp$ if $z \epsilon S_x$.
12. if $S_x$ exists the

$$F_x = \prod_{z \epsilon s_x} F_z^{\Delta_{i,s_x'}(0)}$$

$$= \prod_{z \epsilon s_x} (e(g,g)^{r \cdot q_z(0)})^{\Delta_{i,s_x'}(0)}$$

$$= \prod_{z \epsilon s_x} (e(g,g)^{r \cdot q_z(i) \cdot \Delta_{i,s_x'}(0)}$$

where i = index(z) and $S_x' = \{index(z) : z \epsilon S_x\}$.

13. Return $F_x$
14. else
15. Return $F_x = \perp$
16. end if
17. end if
18. end function
19. A = DecryptNode(CT, $S_k$, R)
20. if $A \neq \perp$ then
21. $A = \frac{e(C,D)}{A} = e(g,g)^{\alpha s};$
22. end if
23. The decryption is performed as follows:

$K' = \tilde{C} / \tilde{A}.$

24. if $e(\sigma, g) = e(H(K)', g^{r_{sn}}$ then
25. The message $K'$ is valid.
26. end if

AP-CBE is used in this system. It is an identity based encryption having one public key and master private keys used to make more restricted private keys. In this private keys have attributes, encryption is done under policy over attributes and can decrypt if attributes satisfies policies.

## IV. EXPERIMENTAL RESULTS:

The Comparative analysis is done on the existing three systems [10], [11] and [14] based on the time taken in milliseconds and file size in kilobytes.

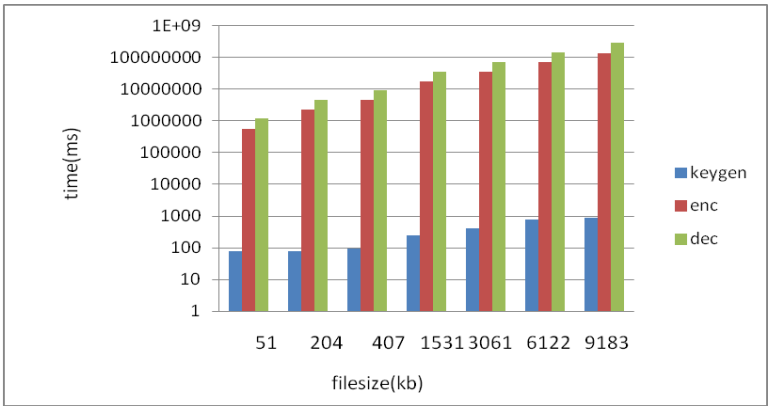


Fig. 4 Computation time(ms) vs file size(kb) of Paillier cryptosystem Algorithm.

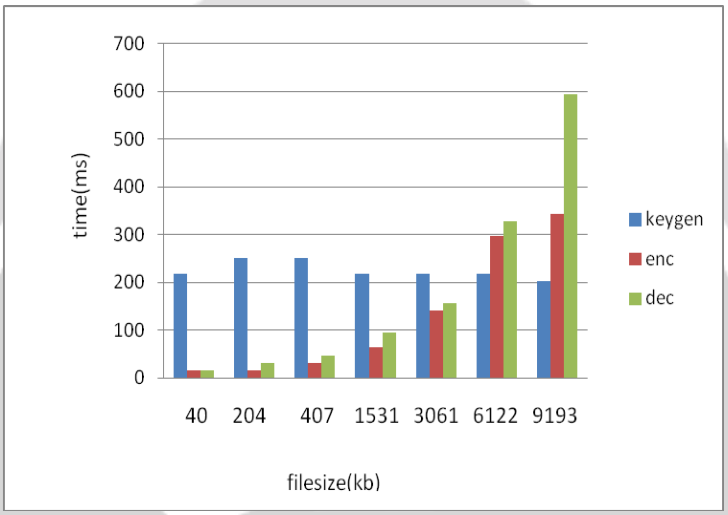


Fig.5 Computation time(ms) vs file size(kb) of AES.

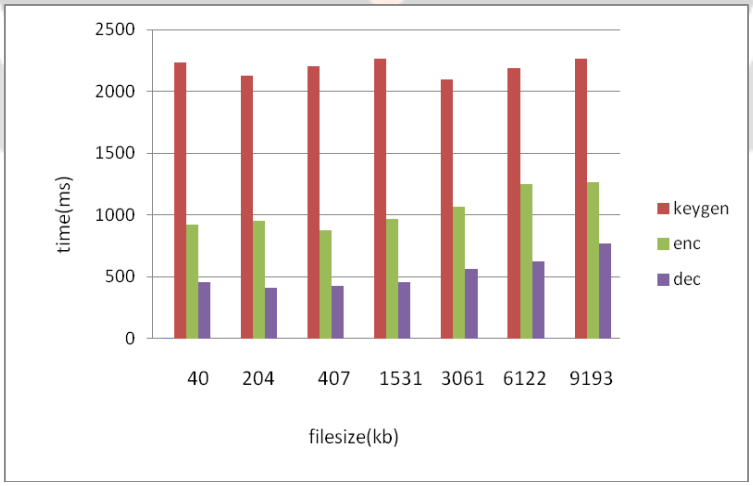


Fig.6 Computation time(ms) vs file size(kb) of CP-ABE and AES

The figure.6 represents the time taken for key generation by CP-ABE and AES for encryption and decryption. Graphical representation of the three system shows data containing file of different sizes takes different time to compute. Based on the application requirement either symmetric or asymmetric algorithm is used.

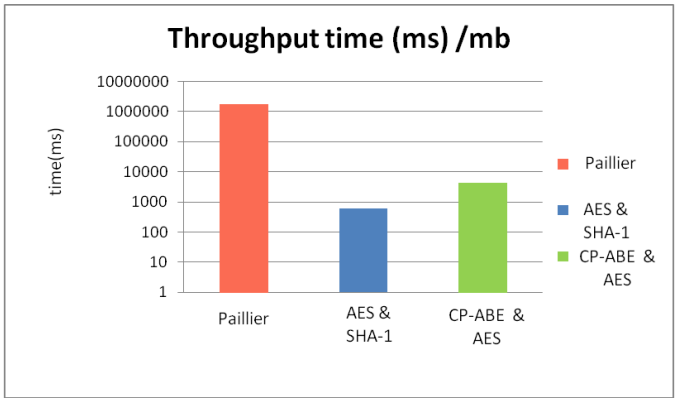


Fig.7 Graphical representation of throughput time for the existing three systems

Experimental analysis proves that symmetric cryptographic algorithm takes much lesser computational time than the asymmetric cryptographic algorithm. Less computation time shows high performance in the system.

## V. CONCLUSION:

In WMSN, security and privacy of Health Monitoring System is mandatory where patient's body conditions are monitored and their information are stored more accurately. Information transmission needs safety and privacy of medical data. Public-key algorithm is computationally higher than symmetric algorithms. Thus Symmetric cryptographic algorithms can be used to provide security while transmitting the sensed data and access control policies are used by cipher-text policy based attribute based signature technique. Hence the privacy and integrity is preserved during the transmission of data in wireless environment.

**REFERENCES:**

1. Moshaddique Al Ameen & Jingwei Liu & Kyungsup Kwak, *"Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications"*, This article is published with open access at Springerlink.com, 12 March 2010.

.

2.Garth V. Crosby, Niki Pissinou, James Gadze, *"A Framework for Trust-based Cluster Head Election in Wireless Sensor Networks"*, IEEE Xplore Conference paper, May 2006 DOI: 10.1109/DSSNS.2006.1.

3. Madhumita Panda, *"Security in Wireless Sensor Networks using Cryptographic Techniques"*, American Journal of Engineering Research (AJER), e-ISSN : 2320-0847 p-ISSN : 2320-0936 Volume-03, Issue-01, pp-50-56, 2014.

4. Prashant Sangulagi1, Mohan G, *"Securing Information in Wireless Sensor Networks"* in IJRET: International Journal of Research in Engineering and Technology eISSN: 2319-1163 | pISSN: 2321-7308, Volume: 03 Special Issue: 03 | May-2014

5. Yao-Tung Tsou, Chun-Shien Lu, *Member, IEEE*, and Sy-Yen Kuo, "*MoteSec-Aware: A Practical Secure Mechanism for Wireless Sensor Networks"* in IEEE Transactions on Wireless Communications, Vol. 12, No. 6, June 2013

6. Vishwa Goudar and Miodrag Potkonjakm, *"A Robust Watermarking Technique for Secure Sharing of BASN Generated Medical Data"*, IEEE International Conference on Distributed Computing in Sensor Systems, 2014 .

7. Snehal M. Gaikwad, Vidya Dhamdhere, *"A Review of Privacy Preserving Techniques in Wireless Sensor Network"*, Network and Complex Systems ISSN 2224-610X (Paper) ISSN 2225-0603 (Online) Vol.4, No.3, 2014.

8. Payal V. Parmar, Shraddha B. Padhar, Shafika N. Patel, Niyatee I. Bhatt, Rutvij H. *Jhaveri "Survey of Various Homomorphic Encryption algorithms and Schemes"* in International Journal of Computer Applications (0975 – 8887) Volume 91 – No.8, April 2014

9. Bhavana D , Chinnaswamy C N, Dr. T H Sreenivas3 *"Maximizing the Lifetime and Data Security of WSNs using HEF Algorithm and Paillier Homomorphism"* in International Journal of Advance Research in Computer

Science and Management Studies Research Article / Survey Paper / Case Study Volume 3, Issue 5, ISSN: 2321-7782 (Online) May 2015 9

10. Xun Yi, Athman Bouguettaya, Dimitrios Georgakopoulos, Andy Song and Jan Willemson, *"Privacy Protection for Wireless Medical Sensor Data"*, IEEE Transactions on Dependable and Secure Computing, DOI 10.1109/ TDSC.2015.2406699, 2015.

11. Daojing He, Sammy Chan, *Member, IEEE*, and Shaohua Tang, *Member, IEEE* "A Novel and Lightweight System to Secure Wireless Medical Sensor Networks" in IEEE JOURNAL OF BIOMEDICAL AND HEALTH INFORMATICS, VOL. 18, NO. 1, JANUARY 2014

12. William Stallings, "Cryptography and Network Security", fifth edition.

13. Behrouz A Forouzan, "Cryptography and Network Security," second edition

14. Chunquiang Hu, Student Member, IEEE, Hongjuan Li, Xiuzhen Cheng, Fellow, IEEE, Xiaofeng Liao, Senior Member, IEEE *"Secure and Efficient data Communication protocol for Wireless Body Area Networks"* in IEEE TRANSACTIONS ON MULTI-SCALE COMPUTING SYSTEMS, VOL., NO., 11, 2015

.