IJCTA, 10(01), 2017, pp. 93-100

A Secure Authentication Technique to Exchange Message between Sensor Nodes in Wireless Sensor Networks

M. Giri* R. Seethalakshmi and S. Jyothi*****

Abstract : Day to day expansion in communication technology helps smart wireless sensor networks to continuously monitoring its applications. In some medicinal applications patient data should be monitor continuously for which sensor deployed in the patient body to collect inpatient therapeutic data. Cost of a sensor node is very cheap in the market and are have limited battery power, and has less memory to store or process data. Due to these limitations sensor networks expect end to end resilient secure and power efficient technique to communicate with other nodes in the networks. In our literature survey we come to know that in existing research work there is a chance to force attacks to capture data which is exchanged from one sensor to other over Wireless Sensor Network (WSN). We proposed a new method to secure exchange of message between sensor nodes, and at the end we proved how our method protect message from various security attacks.

Keywords: Wireless Sensor Networks; authentication method; Sensor Node; Medicinal Data Monitoring; Wireless Applications.

1. INTRODUCTION

The development of communication tools will provide us to use security mechanisms in wireless sensor networks and which will protect data from various security attacks. In medicinal applications sensor nodes are deployed into patient's body by the physician. Wireless sensor nodes are used to continuously monitor patient's record when they moving from one place to other place (home, office, market, shopping, etc) and doctor continuously obtain patient's data like sugar level, BP level, temperature, etc through smart phone devices. Medicinal applications are critical applications and most of the researchers [8], [9] proposed techniques to monitor patient's health conditions through sensor nodes.

With help of TMIS patients will themselves monitor their health conditions, send frequently health reports to physicians over a network. TMIS server maintains all patient records and by verifying patient records physician them self or with consultation of other physician take critical decisions in a different remote locations [14]. TMIS patient data records are useful to physicians as well as patients and which helps to patients reduces both travelling expenses and hospitalization time.

Usages of wireless sensor networks are increased rapidly with population which provides solutions to many applications with optimal cost [7]. Conventional security methods are not suitable for conditional wireless sensor networks. In WSN more number of sensor nodes is deployed into different remote locations

* Associate Professor, Department of Computer Science and Engineering, VELTECH HIGH TECH Dr.Rangarajan & Dr.Sakunthala Engineering College, Chennai, TAMILNADU, India. *prof.m.giri@gmail.com*

** Professor, Department of Computer Science and Engineering, VELTECH HIGH TECH Dr.Rangarajan & Dr.Sakunthala Engineering College, Chennai, TAMILNADU, India. *drseethalakshmi@velhightech.com*

*** Professor, Department of Computer Science, SPMVV University, Tirupati, Andhra Pradesh, India. *jyothi.spmvv@gmail.com*

under different climatically conditions. Main problems with sensor nodes are have limited memory space and battery power. With these conditions we cannot apply conventional security methods and we have to use advanced security methods to protect sensed data from attacks [6].

The remaining sections of this paper outlined as follows. In section II we discussed background study of this work, in section III we present proposed method, in section IV we analyze security analysis of our work with existing method, in section V we completed cost analysis of our work with existing methods, and finally we conclude in section VI.

2. RELATED WORK

WSN has advantages as well as limited with resources, sensor nodes deployed into human body to gather patient's data through internet which results security issues like data integrity should be maintained during transit, establish non breakable connection between patient and server to monitor patient condition and frequently generate patient's statistical report for further treatment.

The researchers Tan.Z et al. [10], proposed secure authentication method for telecare medical system which is useful to monitor patient's health conditions through sensors and authentication method will secure data exchanged between user and telecare server. In their approach they used bio-metric and smart card to provide password based authentication between user and server over WSN. They proved their authentication method protect from various security attacks.

The researchers Yan.X et al. [1], proposed a method for Telecare Medicine Information System (TMIS) which allows both patient and physician to access data or information in remote locations. The authors Tan.Z et al. [10]proposed a bio metric based authentication approach for medical health care system and they proved that their method is away from security attacks. They researchers Yan.X et al. [1] applied cryptanalysis technique on Tan.Z et al. [10]they proved that their method is not protecting from Denial of Service (DoS) attacks.The authors [1] enhanced security futures and they provide solution to resist denial of services attacks.

The researchers Chaturvedi.A[11] proposed remote authentication method for TMIS and which provides data security and data integrity when the data transmitted over WSN channel. The authors Yan.X et al. [1] applied cryptanalysis on Tan.Z et al. [10] and they said that Tan.Z et al. [10] is vulnerable with denial of service attacks and Yan.X et al. [1] proposed enhanced secure method to protect from DOS attack. Chaturvedi.A[11] worked on Yan.X et al. [1] proved that their method is not protecting data from user anonymity attack and password guessing attack. In their method login phase and password change steps are not efficient to verify the input which inturn will provide a chance to force DoS attack. Chaturvedi.A[11] proposed a new method which will remove the problems which are faced by the Yan.X et al. [1] method.

The researchers Lee et al. [12] proposed authentication method by extended work of Zhu et al. for wireless medical sensor networks, they used two mechanisms one is authentication method (password) and the other one is key management method using smart card for TMIS. Authors Das.A.K et al. [13] proved that Lee et al. [12] method is not efficient, because their method has security issues in both authentication and password changing stage. Das.A.K et al. [13] proposed security method which is simply improved version of Lee et al. [12] and cable to solve the design issues which are faced by Lee et al. [12].

In this paper we apply cryptanalysis on Chen.J et al. [3], we will come to know that Chen.J et al. [3] is vulnerable to offline password guessing attack, user impersonation attack, server masquerade attack, and session key framing attack. We propose a new secure authentication technique to exchange message between sensor nodes for healthcare in wireless sensor networks. At the end, we will also done security analysis and cost analysis with other existing algorithms in the same field, and our method is showing better results when compared with existing methods.

3. PROPOSED AUTHENTICATION METHOD

Wireless sensor networks security model consists of sender, sensor nodes, group of sensor node, sink node, communication media, receiver, and opponent. A simple design of such network is depicted in figure 1.

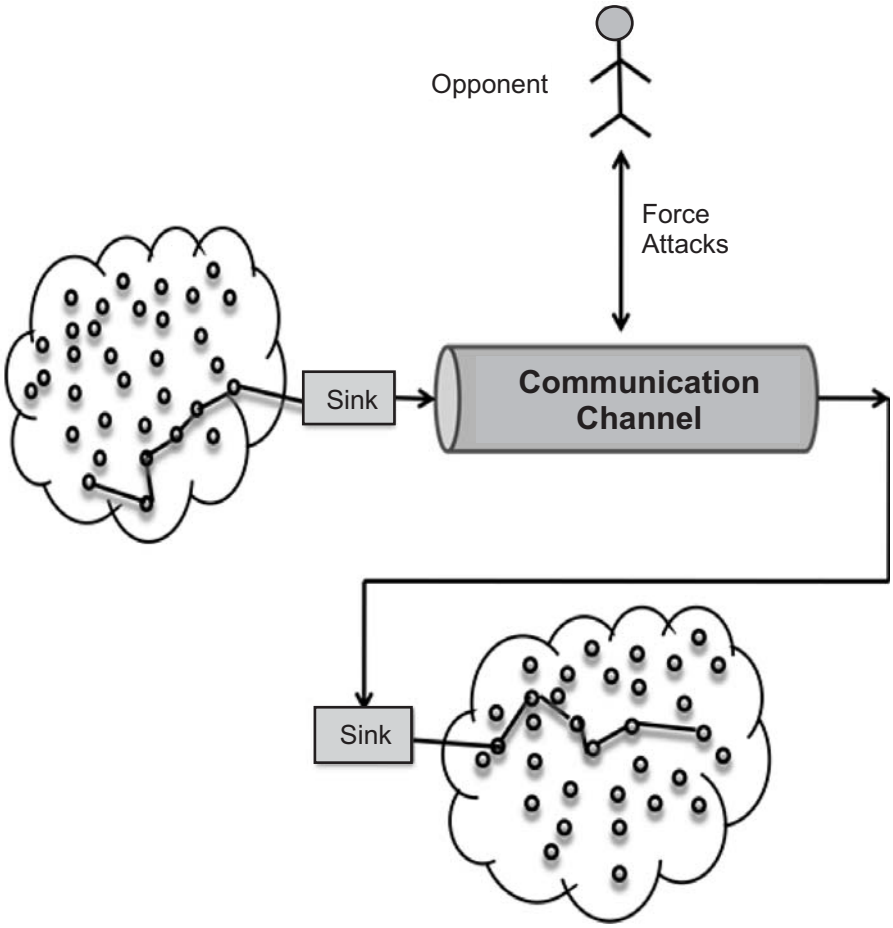

Figure 1: A Simple Wireless sensor network model

We proposed a new novel secure wireless channel to protect from various security attacks. In this model sensor nodes are formed into groups to connect to sink node, each group maintain on sink node to communicate with other sensor node in another group and simple scenario of such network is shown in figure 2. With help of secure communication channel one sensor node communicate message to other node.

In this research paper we proposed improved security mechanism for wireless sensor networks. Proposed model consists of four steps: user registration phase, login phase, authentication phase, and password change phase.

A. User registration phase

Step 1: User U_i send registration request message $\{ID_i, P_{rem\_i} = h(r_i \oplus P_i)\}$ to sensor node through secured channel.

Step 2: Sensor nodereceive user id and password of user then choose a random number r_{sink} for each user and calculate:

$$R = r_{sink} \oplus h(ID_i \,||\, P_{rem\_i}$$
$$C = ID_{sink} \oplus h(P_{rem\_i} \,||\, ID_i)$$
$$N = h(ID_i \,||ID_{sink}||key||r_{sink}) \oplus h(P(_{rem\_i} \oplus ID_i)$$
$$H_i = h(ID_i \,||ID_{sink}||r_{sink}||P_{rem\_i})$$

Sensor node receive authentication ticket for user through secure channel and ticket consists of (Nonce, R, C, H, r_i).

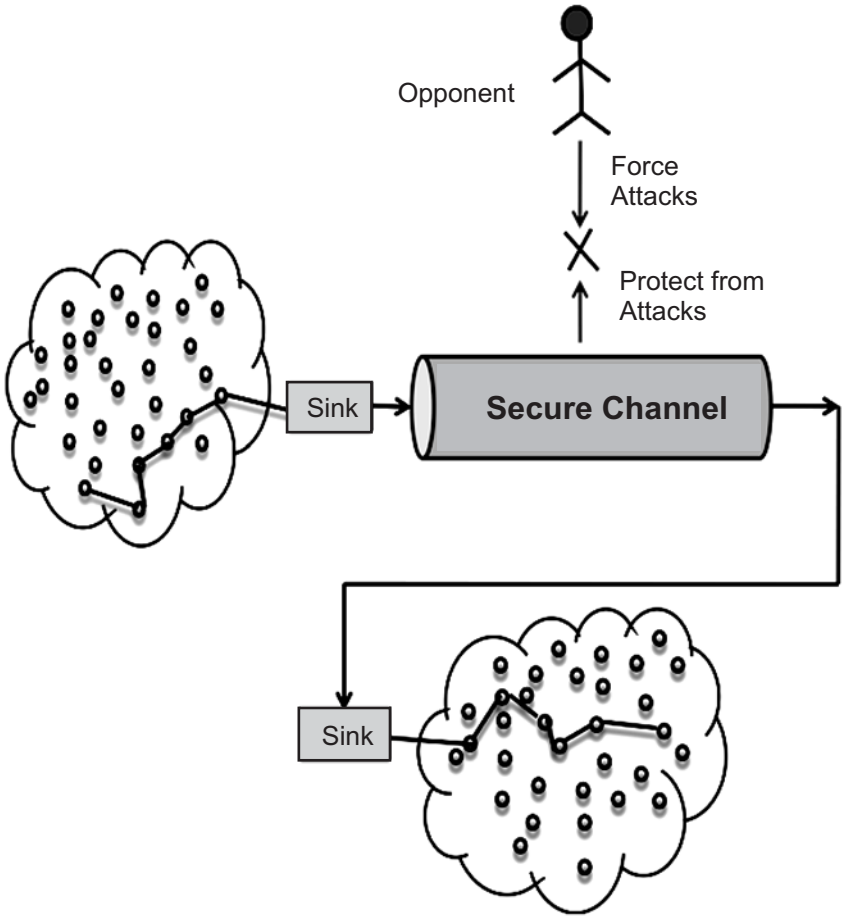

Figure 2: A Simple Wireless sensor network Security

B. Login Phase

Step 1: Userinserts authentication ticket to card reader, user entersID, password, and then ticket reader will perform the following tasks.

Step 2: Calculate remote user password $P_{remi} = h(r_i || P_i)$, get random number r_{sink} from R and ID_{sink} from C.

$$r_{sink} = h(UID_i || P_{remi}) \oplus R$$
$$ID_{sink} = C \oplus h(P_{remi} || ID_i)$$

Step 3: Calculate $H_i^* = h(ID_i || ID_{sink} || r_{sink} || P_{remi})$ and compare H_i^* with H_i if it is equal then authenticated or otherwise user is not authenticated.

Step 4: Prepare login request message $\{ID_{new\_i}, N^*, U_{rem\_i}, H_1, TS_1, S_2, X\}$ and send to sink node.

$$ID_{new\_i} = ID_i \oplus h(r_{sink})$$
$$U_{rem\_i} = r_{rem\_u} \oplus h(ID_i || r_{sink})$$
$$N^* = N \oplus h(P_{remi} \oplus ID_i) = h(ID_i || ID_{sink} || K || r_{sink})$$
$$H_1 = h(ID_i || r_{rem\_u} || r_{sink} || ID_{sink} || P_{remi} || N^* || TS_1)$$
$$S_2 = S_i \oplus h(ID_i || r_{sink})$$
$$X = h(N^*) \oplus P_{remi}$$

C. Authentication Phase

After receiving login request message from user sink node performing the following task to verify user authenticity.

Step 1: Calculate $(TS_2 - TS_1) \leq \Delta t$, where TS_2 is the time of login request message received by sink node, Δt is minimum then only sink node will perform remaining tasks or otherwise simply reject login request message.

Step 2: Sink node get user ID_i from ID_{newi}, calculate N^*, get password P_{remi} from X, S_i from S_2, and r_{rem_u} from U_{rem_i}. Sink node calculate

$$\begin{aligned} ID_i &= ID_{new\_i} \oplus h(r_{sink}) \\ N^* &= h(ID_i \,||\, ID_g \,||K||\, r_{sink}) \\ P_{remi} &= X \oplus h(N^*) \\ r_{rem\_u} &= U_{rem\_i} \oplus h(ID_i \,||\, r_{sink}) \end{aligned}$$

$H_1^* = h(ID_i \,||\, r_{rem\_u} \,||\, r_{sink} \,||\, ID_{sink} \,||\, P_{remi} \,||\, TS_1 \,||\, N^* \,||\, S_2$ & verified with received H_1 from user.

Step 3: Sink node generate random numberr_2, prepare message $\{R_2, N_1, C_2, S_3, TS_2, TS_3, H_2\}$ to sensor node and sent prepared message to sensor node.

$$\begin{aligned} R_2 &= r_2 \oplus h(K_{sink}) \\ N_1 &= N^* \oplus h(K_{sink} \,||\, R_2) \\ C_2 &= r_{rem_u} \oplus h(r_2 \,||\, K_{sink}) \\ S_3 &= S_2 \oplus h(K_{sink} \,||\, r_2 \,||\, TS_2) \\ TS_3 &= TS_1 \oplus h(K_{sink} \,||\, TS_2 \,||\, r_2) \\ H_2 &= h(ID_i \,||ID_{sink}||S_3||r_2||r_{rem\_u}||N^*||TS_2||TS_1) \end{aligned}$$

Step 4: After receiving login request message from sink node sensor node verified message authenticity by calculating H2*. If both H_2 & H_2^* are same then message is authenticated or otherwise message is not authenticated.

$$H_2^* = h(ID_i \,||\, ID_{sink}||S_3||r_2||r_{rem\_u}) \,||N^*||TS_2 \,||TS_1)$$

4. SECURITY ANALYSIS OF PROPOSED METHOD

In this segment we will describe how our method protecting from various attacks like Protecting from offline password guessing attack, Protecting from Impersonation Attack, Protecting from Server Masquerade Attack, Strong mutual authentication, and Refusing Session Key framing by an opponent

A. Protecting from offline password guessing attack

To do security analysis of proposed method first consider same two assumptions discussed in the previous section, we also assuming that communication channel is monitor by the opponent when message is exchanged between sensor node and sink node. An opponent can guess useID_i or password P_i or both but cannot guess sink node secret key (K_{sink}), random numbers, and P_{remi} of 160-bit in length. Therefore in our proposed method with knowing these values opponent cannot frame mathematical equation and our method is protecting password guessing attack.

B. Protecting from Impersonation Attack

To force masquerader attack, opponent must hack login request message and arrange values to form login request. But in table 1 we listed list of values may be hacked and as per the table 1 it is impossible to form login message. Therefore in our method it is not possible to force impersonation attack.

C. Protecting from Server Masquerade Attack

To give the wrong impression like correct sink node, an opponent must calculate and send bogus message to user by knowing $\{UID_i, ID_{sink}, r_{sink}$, etc$\}$ but in our method according to table 1 it is not possible to hake those values and therefore our method is away from Server Masquerade Attack.

D. Strong mutual authentication

In our proposed method, all generated request messages exchange between user and sink node, sink node and sensor node are fully cross verified completely with help of time stamp values and random numbers. As per our discussion in Table 1 it is impossible to attacker to guess all random numbers and time stamp values. Therefore we strongly say that our method provide strong mutual authentication for messages over wireless sensor networks.

E. Refusing Session Key framing by an opponent

In our proposed method XOR operation, hash and concatenation operation are applied every time before exchanging message. Therefore hacking of session key is that much easy. The complete security analysis of proposed method is shown in table 1.

Table 1
Security analysis of proposed method

Mathematical Equation	*Values achievable or known*	*Values not achievable or unknown*
$R = r_{sink} \oplus h(ID_i \| P_{rem\_i})$	None	r_{sink}, ID_i, P_{rem_i}
$C = ID_{sink} \oplus h(P_{rem\_i} \| ID_i)$	ID_{sink}	P_{rem_i}, ID_i
$N = h(ID_i \| ID_{sink} \| key \| r_{sink}) \oplus h(P_{rem\_i} \oplus ID_i)$	ID_{sink}	key, r_{sink}, ID_i, P_{rem_i}
$ID_{new\_i} = ID_i \oplus h(r_{sink})$	None	r_{sink}, ID_i
$N^* = N \oplus h(P_{remi} \oplus ID_i)$	N	ID_i, P_{remi}
$X = h(N^*) \oplus P_{remi}$	None	N^*, P_{remi}
$S_2 = S_i \oplus h(ID_i \| r_{sink})$	S_i	r_{sink}, ID_i
$U_{rem\_i} = r_{rem\_u} \oplus h(ID_i \| r_{sink})$	None	r_{rem_u}, ID_i, r_{sink}
$H_1 = h(ID_i \| r_{rem\_u} \| r_{sink} \| ID_{sink} \| P_{remi} \| N^* \| TS_1)$	TS_1, ID_{sink}	ID_i, r_{rem_u}, r_{sink}, P_{remi}, N^*
$R_2 = r_2 \oplus h(K_{sink})$	None	r_2, K_{sink}
$C_2 = r_{rem\_u} \oplus h(r_2 \| K_{sink})$	None	K_{sink}, r_2, r_{rem_u}
$N_1 = N^* \oplus h(K_{sink} \| R_2)$	None	N^*, K_{sink}, R_2
$S_3 = S_2 \oplus h(K_{sink} \| r_2 \| TS_2)$	TS_2, S_2	r_2, K_{sink}
$TS_3 = TS_1 \oplus h(K_{sink} \| TS_2 \| r_2)$	TS_1, TS_2	K_{sink}, r_2

5. COST ANALYSIS AND DISCUSSIONS

Our proposed research method protects message from security attacks when compare with other related methods. In our proposed method we are not used costly operations like conventional encryption or public key encryption but we used simple concatenation, XOR and hash functions. We compared our proposed method with [1], [2], [3], [4] and comparative results are shown in table 2. The authors Chen. J et al [3], in their paper they represent that time consuming for one symmetric encryption (T_s) is equal to 10 times

time consumed by the hash function ($1T_s = 10T_h$) and The authors [4,5], in their paper they represent that time consuming for one elliptical curve encryption point multiplication (T_{ep}) is equal to 2210 times time consumed by the hash function ($1T_{ep} = 2210T_h$). After complete cost analysis we have shown comparative results in table 3 and our method is performing better when compared with other methods.

Table 2

Comparative analysis of Security attacks with other existing methods

Security Attacks	*Proposed Method*	*[1]*	*[2]*	*[3]*	*[4]*
Protecting from offline password guessing attack	√	X	X	X	X
Protecting from Impersonation Attack	√	X	X	X	X
Protecting from Server Masquerade Attack	√	X	X	X	X
Strong mutual authentication	√	X	X	X	X
Refusing Session Key framing by an opponent	√	X	X	X	X

Table 3

Cost comparison analysis between proposed and existing methods

Phase	*Proposed**	*[1]**	*[2]**	*[3]**	*[4]**
		$* \rightarrow$ *in terms of* T_h			
User registration stage	1	2	1	2	2
Registration stage @sink node	6	2	12	12	2213
User login stage	16	4426	25	25	6636
Login stage @sink node	20	6633	32	53	2215
Login stage @Sensor node	10	4423	22	22	2215
Total cost (hash function)	50	15482	88	110	13277

6. CONCLUSION

At present, we are using sensor devices in many applications which provide wide scope to researchers to develop reliable secure methods for communication over wireless networks. A secure efficient authentication technique is more important in wireless sensor networks for establishing permanent connection to monitor and collect data in critical applications like medicine. In this paper we proposed new authentication method to exchange messages between sensor nodes over wireless sensor networks and we proven how our method is protecting messages from various security attacks. We conduct experiments, security analysis and cost analysis of proposed technique with other existing methods and our method is better than existing methods. Cost wise our method is 55% more capable than Chen et al. [3] and 45% efficient than Lee et al.[2].

7. REFERENCES

1. Yan.X, Li.W, Li.P, Wang.J, Hao.X, and Gong.P, "A secure biometrics-based authentication scheme for telecare medicine information systems", Journal of Medical Systems, Springer, volume 37, Pages 1–6, 2013.
2. Lee.S, Kumar.P, Lee.H, "E-SAP: efficient-Strong authentication protocol for healthcare applications using wireless medical sensor networks", Sensors 12, Pages 1625–1647, 2012.
3. Chen.J, He.D, Kumar.N, Lee.C.C, Chilamkurti.N, Yeo.S.S, "Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks", Journal of Multimedia Systems, Springer, December, 2013.

4. Shi.W, Gong.P, "A new user authentication protocol for wireless sensor networks using elliptic curves cryptography", International Journal of Distributed Sensor Networks, 2012.
5. He.D, Chen.J, Hu.J, "An ID-Based proxy signature schemes without bilinear pairings", Analysis of Telicommunications, volume 66, number 11-12,pages 657-662, 2011.
6. Jain.M.K, "Wireless sensor networks: Security issues and challenges", International Journal of CIT, volume 2, number 1, pages 62-67, 2011.
7. Perrig.S, Warner, "Security in Wireless Sensor networks", Communications of the ACM, Volume 47, Number 6, Pages 53-57, 2004.
8. Fischer.M, Lim.Y.Y, Lawrence.E,Ganguli.L.K, "ReMoteCare: Health Monitoring with Streaming Video", 7thInternational Conference on Mobile Business, Pages 280–286, Barcelona, Spain, 2008.
9. Bellifemine.F, Fortino.G, Giannantonio.R,Gravina.R, Guerrieri.A, Sgroi.M, "SPINE: A Domain-Specific Framework for Rapid Prototyping of WBSN Applications", In Software Practice and Experience, Wiley:Hoboken, NJ, USA, Volume 41, Pages 237–265, 2011.
10. Tan.Z, "An efficient biometrics-based authentication scheme for telecare medicine information systems", Network, volume 2, pages 200–204, 2013.
11. Chaturvedi.A, Dheerendra.M, Mukhopadhyay.S, Kumari.S, Khan.M.K, "Cryptanalysis and Improvement of Yan et al.'s Biometric-Based Authentication Scheme for Telecare Medicine Information Systems", Journal of Medical Systems, Springer, June 2014.
12. Lee.T.F, and Liu.C.M, "A secure smart-card based authentication and key agreement scheme for telecare medicine information systems.", Journal of Medical Systems, volume 37, Springer, 2013.
13. Das.A.K, and Bruhadeshwar.B, "An Improved and Effective Secure Password-Based Authentication and Key Agreement Scheme Using Smart Cards for the Telecare Medicine Information System.", Journal of Medical Systems, volume 37, Springer, September, 2013.
14. Liu.M, Ameen.A, Kwak,K, "Security and privacy issues in wireless sensor networks for healthcare applications", Journal of Medical Systems, Springer, Pages 93–101, 2012.