ISSN: 0974-2115
www.jchps.com Journal of Chemical and Pharmaceutical Sciences

Imposing patient data privacy in wireless medical sensor networks through homomorphic cryptosystems

K.P. Kaliyamurthie*, K. Sivaraman, Ramesh S
Department of CSE, Bharath Univeristy, Chennai
***Corresponding author: E-Mail: kpkaliyamurthie@gmail.com**

ABSTRACT

In recent years, healthcare applications are regarded as hopeful fields for wireless sensor networks, where the patients have been monitored in hospitals and at their accommodating places. These wireless medical sensor networks are more endangered to intruding, modification, eavesdropping, impersonation and playback attacks than the wired networks. A lot of solutions have been developed to secure wireless medical sensor networks. The already available solutions can safeguard the patient data during communication, but unable to terminate the inside attack where the proprietor of the patient database discloses the delicate patient information. In this project, an empirical approach has been presented to safeguard the inside attack by utilizing multiple number of data servers to store patient data for further utility. The main contribution of this work is to distribute the patient information securely in multiple data servers and by employing the homomorphic cryptosystems (modified paillier/elgamal) to accomplish patients' data privacy. This is a secure method against both outside and inside attacks as long as all the data servers are not compromised.

KEY WORDS: Wireless Medical Sensor Networks, Homomorphic Cryptosystems, patient privacy.

1. INTRODUCTION

In recent times, healthcare applications are regarded as hopeful fields for wireless sensor networks, where we can monitor the patients in hospitals and at homes by using these wireless medical sensor networks. Some of the available wireless medical sensor networks are UbiMon, CodeBlue, Mobicare, MEDiSN, Alarm – Net.

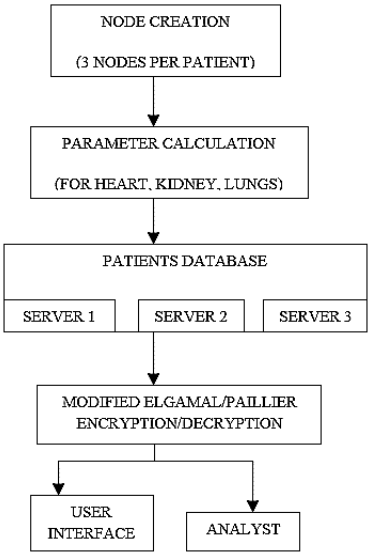

Figure.1.Wireless Medical Sensor Network

This architecture composed of a sensing unit, patient database with three servers, user interface, and analyst interface.

Sensing unit: Sensing unit consists of sensor nodes which senses the patients' health. The patients will worn or implant the sensors which will be sensing the parts such as heart, kidney, lungs, etc.

Patient database: The data collected from the sensors will be stored in the patient's database. The collected information are equally divided by three servers of the database for security reasons.

Analyst interface: Analyst/ doctors can carry out the analysis on the data sensed. Later, gives the result and prescription to the user interface.

User interface: This interface can permit only the legitimate users of the system to query about the data sensed and the results/prescriptions given by the analysts. These wireless medical sensor networks provide a quality of care to the patients without affecting their privacy and comfort.

There are so many security threats in wireless networks than in wired networks. Some of them are eavesdropping, impersonation, modification, intruding, playback attacks.

These security threats are able to capture the patient data from the sensors to know about the condition of the patient. These can be threat to patient data authenticity. Sometimes, while transmitting the patient data to the physician or user, there is a chance for corrupting or altering the data. This could affect the patient.

So, the wireless medical sensor networks to be protected against these various attacks.

Diffie Hellman is one of the public key cryptosystem, which is a method of exchanging keys. But this Diffie Hellman algorithm can't be used for encrypting messages and it is easily liable to man – in – the – middle attacks.

Advanced Encryption Standard is a well known encryption standard based on the principle of substitution permutation. but this standard requires more processing and needs more rounds of communication. This algorithm is easily liable to algebraic attacks.

In a well known asymmetric key encryption algorithm is RSA algorithm. This algorithm can be used for data encryption as well as digital signatures. But, there is a complexity in creating the keys. Since the encryption and decryption requires a lot of calculation, the system gets slow in its speed.

In a FIPS (Federal Information Processing Standard) standard for digital signatures is the Digital Signature Algorithm. This standard has two phases. In the first phase, algorithm parameters will be chosen. In the second phase, the public and private keys for single user has been computed. Entropy, secrecy and uniqueness of the random signature value is more important in this algorithm. It is risky if anyone violate anyone of these three parameters. Because it can disclose the entire secret key to the attacker. In the proposed work, elgamal and paillier cryptosystems have been suggested. These cryptosystems are based on asymmetric algorithm for public key cryptography. These algorithms are composed of key generation, encryption and decryption. These cryptosystems possess homomorphic properties and also provide a semantic security against various attacks. This algorithm increases confidentiality in wireless medical sensor networks. The secret key also can be reused to reduce the computational cost.

Paillier algorithm: Pascal Paillier formulated the paillier cryptosystem, This system consists of key generation, encryption and decryption which has been given as follows:

Key generation:

- Select two large primes a and b
- Calculate the product n = a*b, such that gcd(n,ϕ(n)) = 1, where ϕ(n) is euler function. i.e., ϕ(n) = (a-1) (b-1)
- Then choose a random number g, where g has order multiple of n (or) gcd(L($g^{\lambda} mod\ n^2$), n) = 1, Where L(t) = (t-1)/n and λ(n) = lcm(a-1,b-1).
- The public key (PK) is composed of (g,n), while the private key (SK) is composed of (p,q,λ).

Encryption:

- Encryption of a message m<n is given by: C = $g^m r^n mod n^2$,where random r ϵ Z_N^*

Decryption:

- Decryption of ciphertext c is given by: m = (L($g^{\lambda} mod\ n^2$)/L($g^{\lambda} mod\ n^2$))mod n

Homomorphic property: When decrypted, matches the result of operations performed on the data.Consider the following two cipher texts:

E(x) = E(m_1, pk) = $g^{m_1} {r_1}^n mod\ n^2$

E(y) = E(m_2, pk) = $g^{m_2} {r_2}^n mod\ n^2$

The product of two ciphertexts will decrypt to the sum of their corresponding plaintext.

D(E(x).E(y)) = $m_1 + m_2 (mod\ N)$

The product of a cipher text with another plaintext's generator g will decrypt to the sum of the plaintexts.

D(E(x). g^{m_2}) = $m_1 + m_2 (mod\ N)$

encryption and decryption cannot be completed without knowing the keys

Elgamal algorithm:

Key generation: Generate a cyclic group G, of large prime order f, with generator g.

- Choose a random $x \in \{1, \ldots, f-1\}$ and then compute $t = s^x$
- The public (encryption) key pk is (G,f,s,t).
- The private (decryption) key sk is x.

Encryption:

Let m be a message to encrypt, where $m \in G$

- Choose a random $r \in \{1, \ldots, f-1\}$
- Compute the cipher text c = (X,Y), where $X = s^r$

  $Y = m\, t^r$

Decryption:

- Let c = (A,B) be a ciphertext to decrypt.
- Compute $m = \frac{Y}{X^x}$
- Then the intended message will be given from $\frac{Y}{X^x} = m \cdot \frac{t^r}{s^{rx}} = m \cdot \frac{s^{xr}}{s^{rx}} = m$

These Paillier and Elgamal algorithm is clubbed with hashing for key reuse. This elgamal algorithm also satisfies the homomorphic property. Hashing is the conversion of a message into a key or a value of fixed length that represents the original message of string.

System model: In the proposed method, the sensor senses the patients heart, kidney, lungs and and sends the data to the server. This server divides the patients data equally in three different servers.

The system is given as follows:

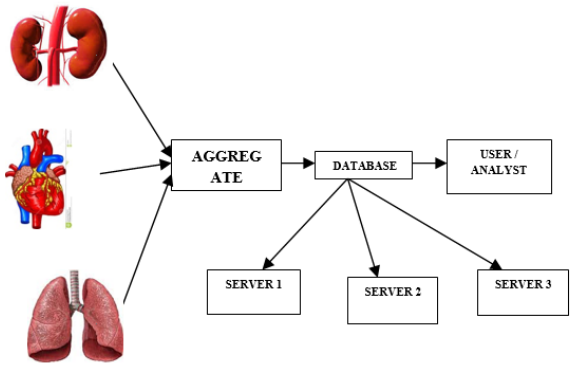

Figure.2.Distributed database model

Consider the patient data "PD_1" which has been distributed equally into three servers S_1, S_2, S_3 via channels α, β, γ respectively.

These three servers and the three channels are completely secure by the use of modified paillier and elgamal cryptosystem.

Consider the medical sensor, which sends a sequence of patient data $PD_1, PD_2, \ldots\ldots$ to three data servers.

Let P_i { $patient \quad ID, \ data \ attribute, \ data \ unit$ }, then medical sensor sends { P_i, α_i} to S_1 through the secure channel for S_1 and similarly sends { P_i, β_i} to S_2 and { P_i, γ_i} to S_3, for i = 1,2,……..Then the system is encrypted using paillier and elgamal cryptosystem.

In this proposed work, the sensors will be sensing the patients heart, kidney, lungs and sends the analysis parameter information such as blood pressure, total cholesterol, partial pressure of gases level, lung volume and capacity, glomerular filteration rate of urea, creatinine, uric acid, etc to the aggregate node. The aggregate node aggregates the collected information and sends to the database.

This database divides the information equally to all the three servers as said earlier. Then paillier/ elgamal algorithm with hashing and homorphic property will be applied to encrypt the data. Then the user or the analysts can get the patient's information safely from the database for further analysis. Only the authorized users/analysts can access the system. Only after the decryption of the servers, the users / analysts can get the patient information for further processing.

As long as the three servers do not put their data together, the privacy of patient data can be protected.

The result of this system model is given in the following. First nodes have been created in the scenario which is shown in fig.3, here three nodes have been considered per patient as each for heart, kidney, lung respectively. The nodes are labeled and shown in the fig. 4.

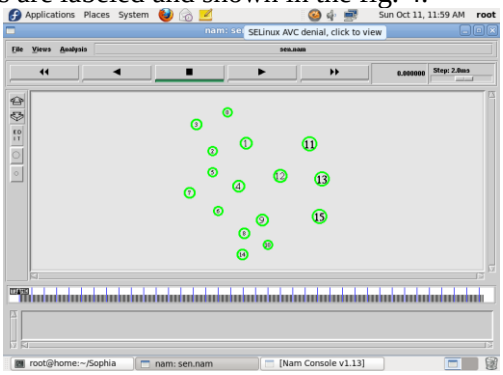

Figure.3. Creation of sensor nodes

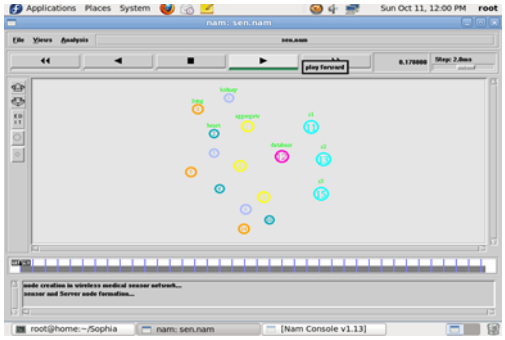

Figure.4. Labeling of sensor nodes

In the above figures 3 and 4, three patients have been considered to be in the scenario and there will be three nodes for each patient to sense their lung, kidney, heart respectively.

Node 2 will be sensing the patient 1's heart, node 3 for lung, node 0 for kidney of patient 1 and sends the gathered information to the aggregate node (node 1) of the patient 1. These has been shown in the following figures 5 and 6. Then the aggregate node of patient 1 will be sending the collected information to the database (node 12), which is shown in figure 7.

Then the database divides the information equally to three servers which are denoted as s1, s2, s3 for security reasons. This has been shown in the following figures 8 and 9.

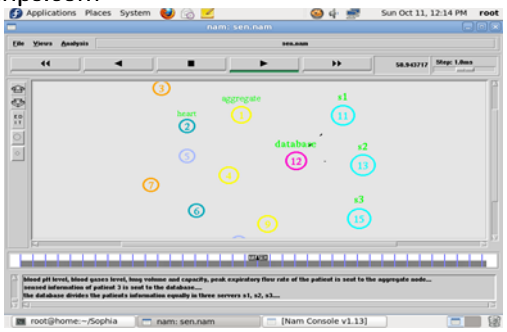

Figure.5. Node 2 senses heart of patient 1 and sends data to the aggregate node

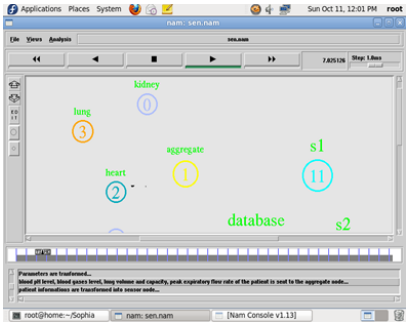

Figure.6. Node 3 senses lung of patient 1 and sends data to the aggregate node

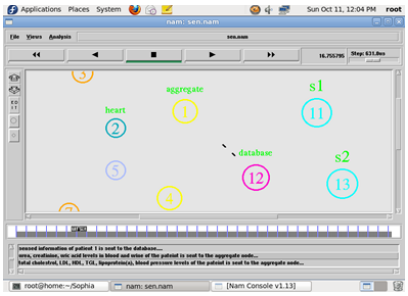

Figure.7.The aggregate node of patient 1 sends data to the patient's database

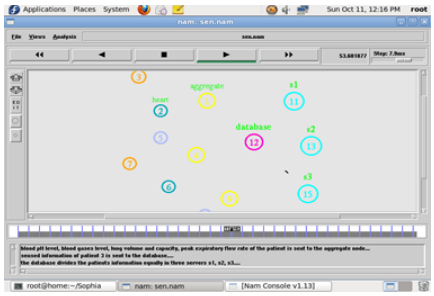

Figure.8.Database sends the data to the servers s1 and s2

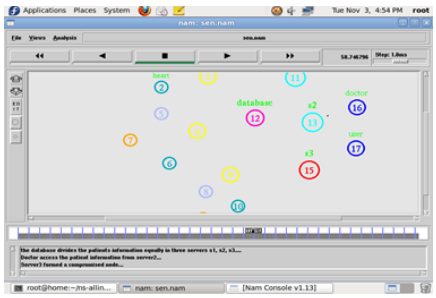

Figure.9.Database sends the data to the server s3

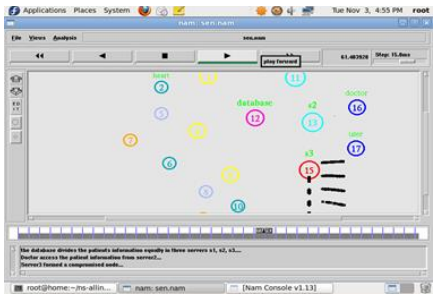

Figure.10.The server s3 becomes a compromised node

Till now, there is no security in the network, so the server s3 get formed as a compromised node and can disclose the patient data to anyone, which is shown in figures 10 and 11.

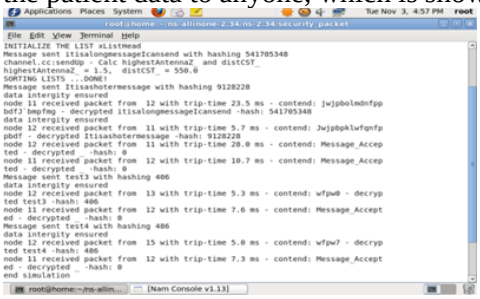

Figure.11.Disclosure of patient information due to the compromised node

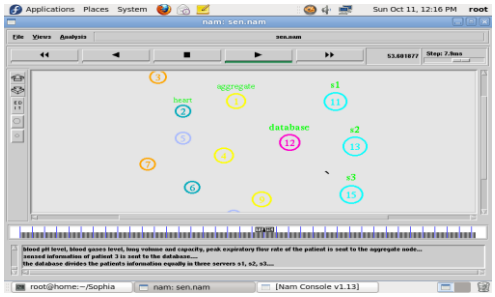

Figure.12.Introduction of security

After the introduction of security, the servers will be secured against all type of attacks. Hereafter the servers can securely transmit the patient information to the users and analysts. This has been shown in figures 12 and 13.

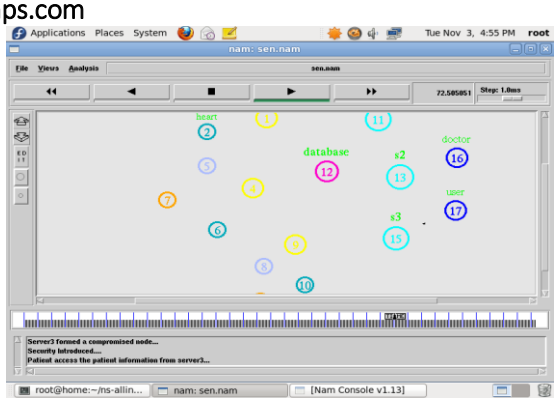

Figure.13. Server sends data to the user promptly without dropping packets after the introduction of the security

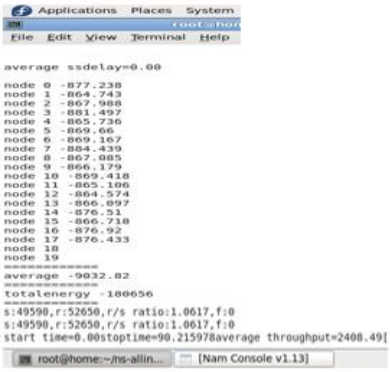

Figure.14. Calculated performance metrics

The performance metrics of the sensor nodes are given as:

- Delay = ending time of transmission – starting time of transmission
- Consumed energy = initial energy - final energy
- Average energy = total energy/number of nodes
- Average throughput = received packet size / (starting time – stopping time of transmission.

The results of the above performance metrics have been shown in the above fig. 14.[32-34]

Sensor nodes sensed the patients heart, kidey and lungs. These analysis are tabulated as follows:

The parameters for kidney analysis in blood and urine level has been given in tables 1 and 2. Parameters for Lung analysis is given in table 3 and the parameters for Heart analysis is given in table 4.

Table.1.Kidney analysis in blood level

Kidney analysis in blood level				
Substances	Patient-1	Patient-2	Patient-3	Normal range
Urea in mg/dl	30	13.5	35	15-40
Creatinine in mg/dl	1.0	0.3	1.3	0.7-1.4 (male) 0.4-1.3 (female)
Uric acid in mg/dl	5	1.5	6	3-7 (male) 2-5 (female)

Table.2.Kidney analysis in urine level

Kidney analysis in urine level				
Substances	Patient-1	Patient-2	Patient-3	Normal range
Urea in g/day	20	12	28	15-30
Creatinine in g/day	1.5	0.5	1.7	1-2
Uric acid in g/day	0.7	0.3	0.65	0.5-0.8

Table. 3. Lung analysis

Parameters	Patient - 1	Patient - 2	Patient - 3	Normal range
Total cholesterol in mg/dl	400	130	150	<200
Low density lipoprotein in mg/dl	150	80	90	<100
High density lipoprotein in mg/dl	30	80	95	>60
Triglycerides in mg/dl	200	110	130	<150
Lipoprotein(a) in mg/dl	19	10	12	<14
Blood pressure in mg Hg	170/110	120/80	130/80	120/80

Thus, the above system model senses the patients heart, kidney and lungs and secures the information by introducing security to the servers against various attacks.

2. CONCLUSION

Thus, this proposed system presented the privacy and security issues in the medical sensor network data collection, storage, queries and provided a privacy preserving network. A light weight homomorphic cryptosystem is used to secure the communication between medical sensors and data servers. Hashing concept has been introduced with these cryptographic algorithms for the key reuse. A new data collection protocol which splits the patient data into multiple servers and stores them in multiple servers respectively. As long as all the data servers gets compromised, the data is secure. Only the legitimate users can access the data servers.

REFERENCES

Nan Li, Langfang, Research on Diffie-Hellman key exchange protocol, second international conference on computer engineering and technology, 4, 2010, 634-637.

Xin Zhou, Xiaofei Tang, Research and implementation of RSA algorithm for encryption and decryption, sixth international forum on strategic technology, 2, 2011, 1118 – 1121.

Digital Signature Standard (DSS). FIPS PUB, 186-4, 2013,

Xun Yi, Athman Bouguettaya, Dimitrios Georgakopoulos, Andy Song, Jan Willemson, Privacy protection or wireless medical sensor data, IEEE transactions on dependable and secure computing, 99, 2015, 1-14.

Mohit P, Biswas G P, Design of elgamal PKC for encryption of large messages, 2nd international IEEE conference publications on computing for sustainable global development, 699-703, 2015.

Mehta N, Jadhav P, Lupane P, Honrao P, Mahalle P, Group authentication using paillier threshold cryptography, 10th international IEEE conference publications on wireless and optical communication networks, 1-4, 2013.

Zhiwei Chen, Ruoquing Zhang, Yatao Yang, Zichen Li, A homomorphic elgamal variant based on BGN's method, IEEE conference publications on cyber ena5bled distributed computing and knowledge discovery, 1-5, 2013.

Kuo Chang Chen, Yu Chi Chen, Gwoboa Horng, A server aided paillier signature generation scheme, 5th international IEEE conference publications on new trends in information science and service science, 2, 222-226, 2011.

Daemen J, Bertoni G, Peeters M, Assche GV, Permutation-based Encryption, Authentication and Authenticated Encryption, DIAC'12, Stockholm, 6 July 2012. Available at http,//www.hyperelliptic.org/ DIAC/slides /Permutation- DIAC2012.pdf

S. Dagtas, G. Pekhteryev, Z. Sahinoglu, H. Cam, N. Challa. Real-Time and Secure Wireless Health Monitoring. Int. J. Telemed. Appl, 2008,

Diffie W and Hellman M, New Directions in Cryptography, IEEE Transactions on Information Theory, 22 (6), 1976, 644-654.

ElGamal T, A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. IEEE Transactions on Information Theory, 31(4), 1985, 469-472.

Malasri K, Wang L, Design and Implementation of Secure Wireless Mote-Based Medical Sensor Network. Sensors 9, 2009, 6273-6297.

Misic J, Misic V, Enforcing Patient Privacy in Healthcare WSNs Through Key Distribution Algorithms. Secure Communication Network, 1, 2008, 417-429.

Montgomery K, Mundt C, Thonier G, Tellier A, Udoh U, Barker V, Ricks R, Giovangrandi L, Davies P, Cagle Y, Lifeguard - A Personal Physiological Monitor for Extreme Environments. In Proc. 26th Annual International Conference of the IEEE EMBS, San Francisco, CA, USA, 2004, 2192-2195,

Ng J, Lo B, Wells O, Sloman M, Peters N, Darzi A, Toumazou C, Yang GZ, Ubiquitous Monitoring Environment for Wearable and Implantable Sensors (UbiMon). In Proc. 6th International Conference on Ubiquitous Computing (UbiComp'04), Nottingham, UK, 2004, 7-14.

Paillier P, Public-key Cryptosystems Based on Composite Degree Residuosity Classes. In Proc. EUROCRYPT, 223-238, 1999.

Raazi S, Lee H, Lee S, Lee YK, BARI+, A Biometric Based Distributed Key Management Approach for Wireless Body Area Networks. Sensors, 10, 2010, 3911-3933.

Ilayaraja K, Ambica A, Spatial distribution of groundwater quality between injambakkam-thiruvanmyiur areas, south east coast of India, Nature Environment and Pollution Technology, 4 (4), 2015, 771-776.

Gopinath S, Sundararaj M, Elangovan S, Rathakrishnan E, Mixing characteristics of elliptical and rectangular subsonic jets with swirling co-flow, International Journal of Turbo and Jet Engines, 32 (1), 2015, 73-83.

Kerana Hanirex D, Kaliyamurthie KP, Kumaravel A, Analysis of improved tdtr algorithm for mining frequent itemsets using dengue virus type 1 dataset, A combined approach, International Journal of Pharma and Bio Sciences, 6 (2), 2015, 288-295.

Thooyamani KP, Khanaa V, Udayakumar R, Efficiently measuring denial of service attacks using appropriate metrics, Middle - East Journal of Scientific Research, 20 (12), 2014, 2464-2470.

Thooyamani KP, Khanaa V, Udayakumar R, Using integrated circuits with low power multi bit flip-flops in different approch, Middle - East Journal of Scientific Research, 20 (12), 2014, 2586-2593.

Thooyamani, K.P, Khanaa, V, Udayakumar, R, Partial encryption and partial inference control based disclosure in effective cost cloud, Middle - East Journal of Scientific Research, 20 (12), 2014, 2456-2459.

Thooyamani KP, Khanaa V, Udayakumar R, Virtual instrumentation based process of agriculture by automation, Middle - East Journal of Scientific Research, 20 (12), 2014, 2604-2612.

Sundar Raj M, Saravanan T, Srinivasan V, Design of silicon-carbide based cascaded multilevel inverter, Middle - East Journal of Scientific Research, 20 (12), 2014, 1785-1791.

Thooyamani KP, Khanaa V, Udayakumar R, Wide area wireless networks-IETF, Middle - East Journal of Scientific Research, 20 (12), 2014, 2042-2046.

Udayakumar R, Kaliyamurthie KP, Khanaa, Thooyamani KP, Data mining a boon, Predictive system for university topper women in academia, World Applied Sciences Journal, 29 (14), 2014, 86-90.

Lingeswaran K, Prasad Karamcheti SS, Gopikrishnan M, Ramu G, Preparation and characterization of chemical bath deposited cds thin film for solar cell, Middle - East Journal of Scientific Research, 20 (7), 2014, 812-814.

Premkumar, S, Ramu, G, Gunasekaran, S, Baskar, D, Solar industrial process heating associated with thermal energy storage for feed water heating, Middle - East Journal of Scientific Research, 20 (11), 2014, 1686-1688.

Gopalakrishnan K, Sundeep Aanand J, Udayakumar R, Electrical properties of doped azopolyester, Middle - East Journal of Scientific Research, 20 (11), 2014, 1402-1412.

Achudhan, M, Prem Jayakumar, M, Mathematical modeling and control of an electrically-heated catalyst, International Journal of Applied Engineering Research, 9 (23), 2014, 23013.

Thooyamani KP, Khanaa V, Udayakumar R, Application of pattern recognition for farsi license plate recognition, Middle - East Journal of Scientific Research, 18 (12), 2013, 1768-1774.