International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-2, July 2019

Confidentiality Protecting Hierarchical Concealed Data Aggregation for Wireless Sensor Network using Privacy Homomorphism

Gaurav Kawade, Nilesh Korde, Kavita Kalambe, Sunita Rawat, Siddhant Jaiswal

Abstract: ***A Wireless Sensor Network is a set of sensor nodes that are integrated with a physical environment. This tiny sensor node capable of sensing physical phenomena and it can process the sense data. Sensor nodes radio range is short so they transfer data in a multihop manner to form network which will send network activities to base station. Data transmission consumes much more energy than computation. So to overcome this problem data aggregation technique can be useful. This approach reduces energy consumption by avoiding repeated data. Security in wireless sensor network is also one of the important issues. Some properties of a WSN make it more harmed by certain types of attackers, compared to traditional wired network. Furthermore, constrained devices create their own problems for wireless sensor network. As sensor node is powered by batteries and node required lot of energy to perform some complex computation. So it is important to prevent every node in computation process which will save energy to gain longer network life. The focus of this work is provides confidentiality protecting hierarchical concealed data aggregation for WSN using privacy homomorphism. End to End Homomorphic Paillier cryptoscheme is used to achieve proposed approach.***

Keywords: ***Wireless sensor networks (WSN), secure data aggregation (SDA), Privacy homomorphism (PH), End to End Encryption, Hope-by-Hope (HBH), Concealed Data Aggregation (CDA)***

I. INTRODUCTION

Wireless sensor network is becoming prominent application of computer science which has increasingly usage in various applications. Wireless sensor network is a diversified network which consists of low-cost tiny devices, called *sensor node*, which will sense environmental parameter such as proximity, temperature, lighting, pressure etc. Then the sense data is forwarded to base station which will be a back end server. At base station data is processed and some information about monitored environment is derived. This data transmission is possible through hop-by-hop wireless data communication where association between sensor nodes is needed to finally transmit sense data to destination node. Wireless sensor networks can be used in various applications such as *Home automation, General engineering*, Agriculture *monitoring, civil engineering, Military applications, Health care etc.*

A. Data Aggregation in WSN

Data aggregation is a dominant part for energy saving in WSN. More power will be consume for scarce and communication between sensor nodes, which will reduce the network lifetime. The sensor node sends the data to data aggregator node and then data aggregator performs some computations on the sense data to produce result. The aggregated data will be forwarded to the destination node as a single observation rather than sending each single sensor node convey their result to the destination and by performing this energy will be saved. The major task of data aggregation is to prevent repeated data transmission which will extend the energy lifetime of WSN. Energy efficiency of a sensor network depends on many other factors such as the data aggregation mechanism, network architecture and the routing protocol. [1] describe the concept of In network aggregation is the task of transferring sense data to base station using a multi hop network and then by using intermediate sensor node , process the data packet.

Different protocols or algorithms are used for data aggregation concept. Following figure show the general data aggregation algorithm work

Revised Manuscript Received on 30 July 2019.
***** Correspondence Author
Gaurav Kawade, Assistant Professor, Department of Computer Science and Engineering, Shri Ramdeobaba College of Engineering and Management, Nagpur, India.
Nilesh Korde, Assistant Professor, Department of Computer Science and Engineering, Shri Ramdeobaba College of Engineering and Management, Nagpur, India
Kavita Kalambe, Assistant Professor, Department of Computer Science and Engineering, Shri Ramdeobaba College of Engineering and Management, Nagpur, India
Sunita Rawat, Assistant Professor, Department of Computer Science and Engineering, Shri Ramdeobaba College of Engineering and Management, Nagpur, India
Siddhant Jaiswal, Assistant Professor, Department of Computer Science and Engineering, Jhulelal Institute of Technology, Nagpur, India

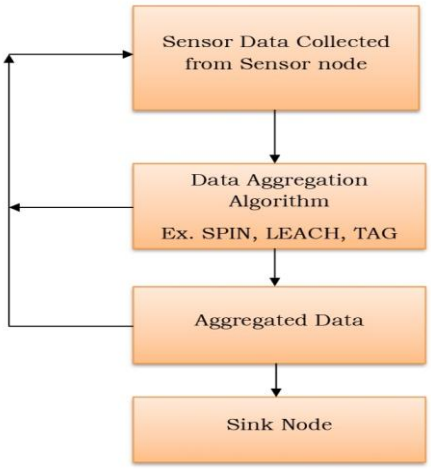

Figure 1: General structure of the data aggregation algorithm

Different data aggregation techniques are available for energy efficiency in Wireless sensor network such as [9]

1. Tree Based Approach

In this approach aggregation tree is constructed which is minimum spanning tree. Base station node believes as a root node while source node as a leaves. Data transfer from leaves node up to base station node. To designing optimal aggregation techniques, this approach can be used.

2. Cluster-Based Approach

In this approach, entire network is fragmented into several clusters and every formed cluster has a one leader called cluster-head. Cluster leader is selected among all cluster members. Cluster leader works as an aggregator node which perform aggregation operation on data received from cluster members and then transmit the aggregated result to base station node.

3. Multi-Path Approach

In this approach all sensor node has multiple route to transmit data to destination node. Through multiple route data packets can be transmitted from source node to destination node and every intermediate node perform data aggregation. If any route fail then data can be transfer from another route so its robust system.

4. Hybrid Approach

This approach can be combination of multipath, tree, cluster scheme. Here base on specific network situation and to some performance statistics data aggregation structure can be adjusted.

B. Security problem in Wireless Sensor Network

In wireless sensor networks message authenticity, confidentiality, and integrity are main concerns. In traditional network those concerns are handled by using symmetric cryptographies. The drawback of symmetric cryptography is that sender and receiver have to share the common secret key before data transferring. In asymmetric cryptography the issue of interchanging shared secret keys is solved by using security protocols like IPSec, SSH, SSL. Because of limited processing of sensor node such type complex asymmetric cryptographic operation is very challenging task in WSN. [11]

C. Motivation

If the base station node of data aggregation is compromised, an attacker will have control on sense data of all sensors. If attacker succeeds to compromise the aggregator which is nearer to destination node then he could perform Denial of service attack or change the aggregation data. Implementation of some sort of robust aggregation is required in order to reduce effect of compromised sensor nodes. Attacker can compromise the aggregator node or compromised sensor node which has involvement in aggregated result. By designing some security technique such type of attacks can be stop in WSN.

II. RELATED WORK

The secure data aggregation was presented by [2] who studied the issue of data aggregation when only one node is compromised. In this technique sense data are forwarded unchanged without aggregating them at the immediate next hop, it is aggregated at the second hop. In this technique the sensor needs to store sense data to authenticate it when base station revealed the shared key.

The issue of aggregating encrypted data in wireless sensor network was studied by [3] and then refined in [4]. The researchers introduced to make use of homomorphic encryption technique to perform arithmetic operations over ciphertexts data and this data need to be transfer in a multi-hop manner. Because of less security level, as it is protected against ciphertext-only attacks only. In [4] author introduced a scheme may be provably secure but it has the disadvantage that the aggregating base station node knows which sensor node were participated in the data aggregation operation, for regenerating the key-streams which is required for decryption operation. In [5] [6] authors introduced a framework of data authentication for hierarchical topology ad hoc sensor networks. Another approach which deals with plausible data aggregation is introduced in [7] and SIA in [8]. The main goal for computing plausible aggregation data was the efficiency accuracy trade-off.

Problem of encrypted data aggregation in the wireless sensor network is being discussed in [13]. The presented protocol Concealed Data Aggregation which use homomorphic encryption technique that performs aggregation on encrypted data. Here, the security level is still reasonable and the PH [14] helps to perform encryption in the wireless sensor network, even though [12] introduced that PH is not secure for plain text attacks.

A. Research Objective

The main objective of this research paper is to address the security problem of data aggregation in WSN. The aim is to implement and perform simulation result evaluation of a secure data aggregation technique that carry out the additive Homomorphic cryptographic operation on sense data which will protect against various security attacks such as data confidentiality, and securely perform the data aggregation. This scheme provides the confidentiality for data aggregation in WSN with help of End to End Homomorphic Paillier cryptoscheme.

III. MATHEMATICAL PRELIMINARIES

Wireless sensor network has several properties which is common with the traditional wireless networks. The requirements for data security in the wireless sensor network are also similar to traditional wireless networks [6]. The security requirements for data aggregation protocols to make it attack-resistant are Data Confidentiality, Data Integrity, Data Freshness, Data Availability and Authentication.

A. Public Key Based Cryptoscheme for Data Concealment in WSN

In this work, we consider WSNs in which confidentially message is transfer. It is our aim to prevent eavesdropping data communication between the source node, aggregator node, and base station node. By performing encryption operation on transmitted data this can be achieved.

B. Privacy Homomorphism

In [10] privacy homomorphism (PH) technique an encryption operation can be performed on encrypted data. Let M and N represents two rings, × denote multiplication and + denote addition. Consider K as a keyspace. Let represent an encryption transformation $E : K \times M \to N$ and the decryption transformation $D: K \times N \to M$.

Given $a, b \in M$ and $k \in K$ we term

$$a + b = D_k(E_k(a) + E_k(b))$$

Additively homomorphic and

$$a \times b = D_k(E_k(a) + E_k(b))$$

Multiplicatively homomorphic. Initially work on Privacy homomorphism was done in a seminal paper by [15]. Generally, the more operands a PH supports the more computation intensive the transformations E and D.

C. Aggregation of Encrypted Data

In end-to-end data preserving aggregation technique every sensor node encrypts their sensed data with the help of encryption algorithm. In additive homomorphic scheme, data is added as they are transmitted towards the base station. The base station decrypts the aggregate data and derives certain informational data.

Domingo-Ferrer's approach can be apply for passive attacker to conceal the process of data aggregation in a WSN:

Sensors node S_1 to S_n perform encryption on their sense data s_1 to s_n such that

$s'_1 = E_{(r,g')}(s_1)$ to $s'_n = E_{(r,g')}(s_n)$ before forwarding data to the node A. Then, node A performs operation on the encrypted data by applying some function and evaluate

$y' = f(s'_1, \ldots\ldots, s'_n)$. Afterward, the aggregator node A transmits

y' to the R which will decrypts the y' and derives the gathered data $y = D_{(r,g')}(y')$. Figure 2 illustrates the above approach. [11]

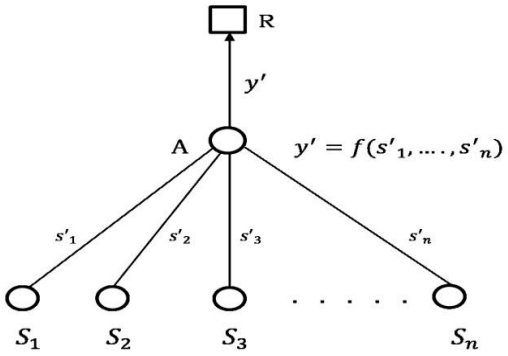

Figure 2: Data Aggregation using Privacy Homomorphism [11]

D. Homomorphic Tallying with Paillier Cryptosystem

Paillier cryptosystem

French researcher Pascal Paillier invented an algorithm for public key cryptography in 1999 and this algorithm is known as Paillier Cryptosystem.

The important thing in this technique is use of asymmetric key algorithms for public key cryptography, where the key used to encrypt a message is not the same as the key used to decrypt it. Every user has a pair of cryptographic keys a *private* key and a *public* key. The public key is widely distributed so anyone can use it while the private key is kept secret. The messages which sender wants to send first it is encrypted with the recipient's public key and then it can only be decrypted with the corresponding private key of receiver. The keys are related mathematically, but the private key cannot be feasibly (i.e., in actual or projected practice) derived from the public key [15].

The Algorithm works as follows:

Key generation

1. Select randomly any two large prime numbers *p* and *q* and independently of each other such that $\gcd(pq, (p-1)(q-1)) = 1$

This property is assured if both primes are of equivalent length, i.e., $p, q \in 1 \parallel \{0,1\}^{s-1}$ for security parameter *s*.

2. Compute RSA modulus $n = pq$ and Carmichael's function $\lambda = lcm(p-1, q-1)$ it can be computed using $\lambda = \frac{(p-1)(q-1)}{\gcd(p-1,q-1)}$

3. Select generator *g* where $g \in \mathbb{Z}^*_{n^2}$ there are two ways of selecting the g.

a. Randomly select g from a set $\mathbb{Z}^*_{n^2}$ where

$$\gcd\left(\frac{g^{\lambda} \bmod n^2 - 1}{n}, n\right) = 1$$

There are $\Phi(n) * \Phi(n)$ number of valid generators, therefore the probability of choosing them out of $n\Phi(n)$

elements of $\mathbb{Z}_{n^2}^*$ set is relatively high for big n.

b. Select α and β randomly from a set $\mathbb{Z}_n^*$then calculate

$$g = (\alpha n + 1)\beta^n mod\, n^2 .$$

4. Calculate the following modular multiplicative inverse

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

Where the function *L* is defined as $(u) = \frac{u-1}{n}$. If valid generator was selected then only this multiplicative inverse exists

• The public (encryption) key is (n, g).

• The private (decryption) key is (λ, μ).

A simpler variant of the above key generation steps would be to set $g = n + 1, \lambda = \Phi(n)$ and $= \Phi(n)^{-1} \, mod \, n$,

where $\Phi(n) = (p-1)(q-1).$

Encryption

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

Decryption

1. Ciphertext $c \in \mathbb{z}_{n^2}^*$
2. Compute message:

$$m = L(c^\lambda \, mod \, n^2) \cdot \mu \, mod \, n$$

Homomorphic properties

The important feature of the Paillier cryptosystem is its homomorphic properties. As the encryption function is additively homomorphic, the following identities can be described:

• **Homomorphic addition of plaintexts**

The product of two ciphertexts will decrypt to the sum of their corresponding plaintexts,

$$D(E(m_1, r_1) * E(m_2, r_2) \, mod \, n^2) = m_1 + m_2 \, mod \, n$$

The product of a ciphertext with a plaintext raising g will decrypt to the sum of the corresponding plaintexts,

$$D(E(m_1, r_1) * g^{m_2} \, mod \, n^2) = m_1 + m_2 \, mod \, n$$

Practically, this leads to the following identities: Where ∀ $\boldsymbol{m1}$, ∈ $\mathbb{Z}\boldsymbol{n}$ and $\boldsymbol{k} \in \mathbb{N}$

$$D(E(m_1)E(m_2) \, mod \, n^2) = m_1 + m_2 \, mod \, n$$
$$D(E(m)^k mod \, n^2) = km \, mod \, n$$
$$D(E(m_1)g^{m_2} \, mod \, n^2) = m_1 + m_2 \, mod \, n$$

$$D(E(m_1)^{m_2} mod \, n^2) = m_1 m_2 \, mod \, n$$
$$D(E(m_2)^{m_1} mod \, n^2) = m_1 m_2 \, mod \, n$$

IV. SIMULATION RESULT

The results are from extensive simulations of an event-driven data sensor network. A packet-level simulator is used to explore the performance of the proposed schemes under various traffic conditions. The main purpose of our experiments is to examine whether the proposed secure data aggregation by end to end homomorphic paillier cryptoscheme module can provide accurate results, and whether such model can provide the additional lifetime-savings over other schemes.

A. Simulation Overview

A typical simulation with ns and the mobility extension is shown in Figure 3. In this two input files are generated to ns simulator:

- To describe the movement pattern of the nodes, scenario file is generated.
- To describe the traffic in the network, communication file is generated.

The above files can be generated by drawing them by hand with the help of visualization tool or by generating completely randomized movement and communication patterns with a script.

These files are then used for the simulation and as a result from this, a trace file is generated as output. Prior to the simulation, the parameters that are going to be traced during the simulation must be selected. The trace file can be used to scanned and analyzed for the various parameters that we want to measure. This can be used as data for plots with for instance Gnuplot. The trace file can also be used to visualize the simulation run with Network animator. [14].

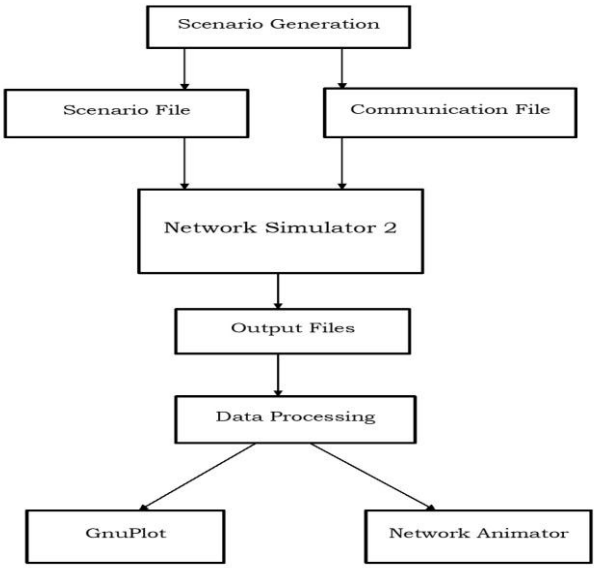

Figure 3: Simulation Overview [14]

B. Results and Discussion

This section presents the output of the simulation. The cryptography algorithm is responsible for security performance of wireless sensor network. We have used Paillier Homomorphic cryptoscheme algorithm to transfer the secure data packets between the nodes. NAM is tcl/tk based animation tool that provides animation or Nodes, Links, Queues, Packets and Agents. The figure 4 shows the NAM output of the simulation where nodes are deployed with static tree topology.

Figure 4: NAM output for Wireless Sensor Simulation

In this figure, 15 nodes are shown out of which one is base station, eight are leaf node and others are aggregator node. Here Base Station is sink node which has private key for decryption of encrypted data which was received from its child. Leaf node encrypts the sense data by using the public key and sends it to its respective parent which can be aggregator node. Aggregator node received encrypted data from its all child but can't decrypt it because it don't have private key. So, aggregator nodes perform the aggregation function on encrypted data and pass this data to its parent and so on. Finally when base station received encrypted data from its child it decrypts it by using private key and get the plaintext.

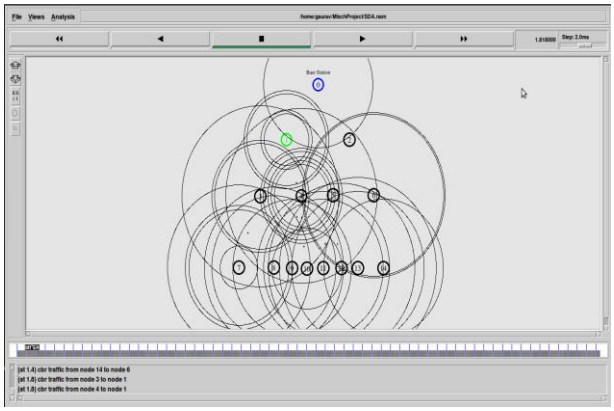

Figure 5: NAM output for Transmitting data to parent

In figure 5, leaf node transmitting encrypted data to its parent. For encryption Pailliers hommomorphic cryptoscheme is used which is a public key based cryptoscheme. In this simulation all sense data and its encryption by using paillier cryptoscheme is saved in encryption txt file. This encryption file will also shows the sum of sense data. Encryption on sense data is performed as shown in section III D. Figure 6 shows the encryption text file of sense data.

	Plaintext	Cyphertext
node_(0)	6	676
node_(1)	13	11335
node_(2)	3	6099
node_(3)	1	33027
node_(4)	16	5912
node_(5)	12	24799
node_(6)	15	19376
node_(7)	7	22181
node_(8)	12	24799
node_(9)	14	32840
node_(10)	2	19563
node_(11)	13	11335
node_(12)	6	676
node_(13)	3	6099
node_(14)	13	11335

Total Sum : 136

Figure 6: Encryption of sense data.

Next, aggregator node performs the aggregation function such as sum on encrypted data. Paillier cryptoscheme has property that if we multiply the encrypted data then it is equivalent to addition of plaintext data. So, by using this property every aggregator node perform multiplication of encrypted data and send result to parent. Figure 7, show result of aggregator node multiplication of encrypted data.

```
num_nodes is set 15
INITIALIZE THE LIST xListHead

Traffic: cbr
Acknowledgement for data: on

 Plaintext : 136
Agg3: 18167050225713
Agg4 :3798158015040
Agg1 : 782130046355869526672281099200
Agg5 :190021345540
Agg6 :1339504829040
Agg2 :155240597631623013707127840O
Agg0 : 8207879501562751701307392244797859057821992593748228812800O0
Decrypt: 136

Starting Simulation...
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 35.5
SORTING LISTS ...DONE!

Transmitting data ...


NS EXITING...
```

Figure 7: Multiplication of encrypted data at Aggregator node

```
Cyphertext : 8207879501562751701307392244797859057821992593748228812800O0

Plaintext : 136
```

Figure 8: Decryption file at base station.

Finally, base station received the encrypted data from its child.

It is very large digit data which is in encrypted form. By using private key in paillier cryptoscheme algorithm we will get original data which is sum of all sense data. Decryption is done as shown in section III D. Figure 8 is showing the decryption text file.

V. CONCLUSION AND FUTURE WORK

The work provides confidentiality protecting hierarchical concealed data aggregation for WSN using privacy homomorphism. Simulation study is performed and examines the simulation environment for wireless sensor network. Various features of NS2 is seen with encryption/decryption function. Then simulation overview is shown. In result and discussion simulation of proposed approach is studied and examined. The work discussed in this paper highlights several open problems and areas of future research such as continuation of this work includes the support of other privacy homomorphism in data aggregation and impact of the scheme on the different types of the network, Develop a new methods for providing data Integrity in data aggregation in wireless sensor network and Develop new methods for authenticity in data aggregation in wireless sensor network

REFERENCES

1. E. Fasolo, M. Rossi, J. Widmer, and M. Zorzi. "*In-Network Aggregation Techniques for Wireless Sensor Networks: A Survey*". In IEEE Wireless communication 2007
2. L. Hu and D. Evans. "*Secure aggregation for wireless networks*". In 'SAINT Workshops', IEEE Computer Society, 384–394, 2003
3. J. Girao, D. Westhoff, and M. Schneider. "*Cda: Concealed data aggregation for reverse multicast traffic in wireless sensor networks*". In IEEE International Conference on Communications (ICC2005), Seoul, Korea, May 2005
4. C. Castelluccia and E. Mykletun and G. Tsudik. "*Efficient Aggregation of encrypted data in Wireless Sensor Networks*". Mobile and Ubiquitous Systems: Networking and Services, 2005.
5. Bohge, M., Trappe, W. "*An Authentication Framework for Hierarchical Ad Hoc Sensor Networks*". In 2nd ACM Workshop on Wireless Security (WiSe'03), 79-87, September 2003.
6. A. Perrig, R. Szewczyk, V. Wen, D.E. Culler, J.D. Tygar. "*SPINS: Security protocols for sensor networks*". In Mobile computing and Networking, 89-199, 2001
7. Boulis, A., Ganeriwal, S., Srivastava, M.B. 2003. "*Aggregation in sensor networks: an energy-accuracy trade-off*". In Elsevier journal of Ad Hoc Networks, Volume 1, Issues 2-3, 317-331, September 2003.
8. Przydatek, B., Song, D., Perrig, A. 2003. "*SIA: Secure Data Aggregation in Sensor Networks*". In 1st ACM Workshop on Sensor Systems (SenSys'03), November 2003.
9. Jadia, P. & Mathuria, A. 2004. "*Efficient secure aggregation in sensor networks*". In L. Boug´e & V. K. Prasanna, eds, 'HiPC', Vol. 3296 of Lecture Notes in Computer Science, Springer, 40–49, 2004.
10. Wagner, D. 2003. "*Cryptanalysis of an Algebraic Privacy Homomorphism*". (Revised version), In Proceedings of the 6th Information Security Conference (ISC03), Bristol, UK, October 2003.
11. Westhoff, D., Girao, J. & Acharya, M. "*Concealed data aggregation for reverse multicast traffic in sensor networks: Encryption, key distribution, and routing adaptation*". IEEE Transactions on Mobile Computing 05(10), 1417–1431, 2006.
12. Domingo-Ferrer, J. 2002. "*A provably secure additive and multiplicative privacy homomorphism*". In Information Security Conference, LNCS 2433, 471-483, 2002.
13. Paillier, P. 1999. "*Public-key cryptosystems based on composite degree residuosity classes*". In Advances in Cryptology (EUROCRYPT '99), vol. 1592 of Lecture Notes in Computer Science, 223–238, Springer, New York, NY, USA, 1999.
14. Tony Larsson and Nicklas Hedman 1998. *"Routing Protocols in Wireless Ad-hoc Networks - A Simulation Study".* Master's thesis in Computer Science and Engineering, Lulea University of Technology Stockholm, 1998.
15. Rivest, R.L., Adleman, L., Dertouzos, M.L. *"On data banks and privacy homomorphisms". In Foundations of Secure Computation, Academia Press, 169-179, 1978.*

AUTHORS PROFILE

Gaurav Kawade has received Master of Technology degree in computer Science and Engineering from Visvesvaraya National Institute of Technologyisv.Nagpur in 2015. Presently he is working as an Assistant Professor at Shri Ramdeobaba College of Engineering and Management, Nagpur. His research areas are Wireless Sensor Network, Network Security, parallel computing. He has published research papers in National and Internal Journals and has 2 conferences proceeding in Scopus Indexed journal.

Nilesh Korde has received Master of Technology degree in Information Technology from YCCE an Autonomous Institute at Nagpur University India in 2014. Presently he is working as an Assistant Professor in Computer Science and Engineering Department at Shri Ramdeobaba College of Engineering and Management Nagpur (An Autonomous Institute). He has published research papers on Parallel Computing, IOT, Cache Management and Clustering. Recently he is working on Natural language Processing, Data Retrieval and Machine Learning.

Kavita Kalambe currently working as Assistant Professor in the Department of CSE at SRCOEM. She received B. E. degree from KDK college of engineering, Nagpur in 2010 and M. Tech degree in CSE specialization from G. H. R. I. E. T. W. Nagpur, Nagpur University in 2015. Her current research interests include Algorithm designing, High Performance Computing Architecture, Wireless Sensor Network, Microprocessor and Microsystems.

Sunita Rawat presently working as a Assistant professor in Computer Science and Engineering department and pursuing my PhD in the field of NLP. I have some publications in National and International Conferences. and have 2 publications in Scopus Indexed journal. I have ISTE membership.

Siddhant Jaiswal has received Master of Technology degree in Computer Science and Engineering from SRCOEM an Autonomous Institute at Nagpur University India in 2013.Presently he is working as an Assistant Professor in Computer Science and Engineering Department at Jhulelal Institute of Technology, Nagpur. He has published research papers on Networking, VANET, Parallel Computing and IOT. Recently he is working on IOT, Machine learning and Blockchain.