A Secure Data Transmission Scheme using Asymmetric Semi-Homomorphic Encryption Scheme

S. Nagavalli[1], G.Ramachandran[2]
[1]Department of Computer and Information Sciences, Annamalai University, Annamalainagar –608 002, Tamil Nadu, India.
[2]Department of Computer Science & Engineering, Annamalai University, Annamalainagar –608 002, Tamil Nadu, India.

Article Info

Article history:

Received May 28, 2018
Revised Jul 26, 2018
Accepted Aug 21, 2018

Keyword:

Homomorphic Encryption
Symmetric Cryptosystem
Wireless Sensor Network

ABSTRACT

The compressive detecting based information accumulation accomplishes with high exactness in information recuperation from less inspection which is available in sensor nodes. In this manner, the existing methods available in the literature diminish the information gathering cost and delays the existence cycle of WSNs. In this paper, a strong achievable security model for sensor network applications was initially proposed. At that point, a secure data collection conspire was displayed based on compressive detecting, which improves the information protection by the asymmetric semi-homomorphic encryption scheme, and decreases the calculation cost by inadequate compressive grid. In this case, particularly the asymmetric mechanism decreases the trouble of mystery key circulation and administration. The proposed homomorphic encryption permits the in-arrange accumulation in cipher domain, and in this manner improves the security and accomplishes the adjustment in system stack. Further, this paper focuses on estimating various network performances such as the calculation cost and correspondence cost, which remunerates the expanding cost caused by the homomorphic encryption. A real time validation on the proposed encryption scheme using AVISPA was additionally performed and the results are satisfactory.

Copyright © 2018 Institute of Advanced Engineering and Science.
All rights reserved.

Corresponding Author:

S. Nagavalli,
Department of Computer and Information Sciences,
Annamalai University,
Annamalainagar–608 002, Tamil Nadu, India.
Email: nagavalli52@gmail.com

1. INTRODUCTION

Wireless Sensor Networks (WSN) has been deployed in different applications which include personal, business and military regions. It comprises of bunches of minimal effort and battery controlled hubs, which are regularly circulated in unattended conditions. Secure information accumulation has been proposed as a pivotal way to deal with settling the vitality and security challenges. The compressive detecting based information accumulation [1-3], which join information procurement with information pressure, can outperform the limits of the customary hypothesis by investigating the sparsity of compressible signs. It accomplishes high accuracy information recuperation from less testing information, and in this way diminishes the information accumulation cost and draws out the existence cycle of WSNs.

In recent times, most of the sensor hubs can't avoid assaults and are anything but difficult to catch, so hubs are not appropriate for put away private data. Even attackers with their assault models are efficient; the enemy traded off a hub initially, and afterward actualized the assault to get the estimation grid. In order to secure the sensor network, various minimal encryption schemes have been proposed. Numerous works on sensor crypto system are being carried out [5, 6] based on the randomized estimation of security conservation. The Symmetric Cryptosystem [4] was first clarified as a single key cryptosystem, where the pseudo-random estimation framework was used as the key, and the estimation result is the figure content of unique signs. It is a light-weight encryption plot. The encoding step and the recouping step can be translated as the encryption and the unscrambling separately, and along these lines no additional computational cost is required. The controllable occasion activating assault situation is just changed the estimation of one hub, which means the irregular occasion activating assault model has been changed and all the assaults are targeted to specific nodes. Hence, the existing encryption system which uses the typical private (mystery) key cannot be reused. In order to address the above mentioned issues, this paper proposes a novel homomorphic encryption scheme. The key idea is to guarantee the refresh of key and proof based hash capacities, which assumes the nodes are secure by themselves. The contribution of this paper is as follows:

1. Proposed a minimalistic encryption standard which supports all the sensor network model.
2. Compressive detecting based encryption scheme with support to optimal securing strategy.
3. A secure proof based on hash capacities which assumes the nodes are secure.

The rest of this paper is organized as follows: Section II discusses the state of the art methods on homomorphic encryption schemes. Section III deals with the proposed encryption scheme. Section IV discusses about the experimentation of encryption schemes. The penultimate section of this paper discusses about the performance analysis and finally the paper is concluded.

2. LITERATURE SURVEY

In this section, various state of the art techniques available in the literature are discussed. This section dissects into three phases namely i) Obscurity ii) Directing consolidated plan iii) Destructive modification.

2.1. Obscurity

In the obscurity based plan, a straight change is connected to the first information, where the change grid is the arbitrary grid. This straight change is deciphered as a lightweight symmetric encryption plot, where the arbitrary grid is the private key. In the compressive detecting encryption plans [7, 8, 11], the vector size of the change comes about is substantially less than that of the first information, which implies the first information is packed amid the change. In the randomize change based plan [9, 10], the confusion change is connected to the compressive estimation comes about, and the vector size of the estimation comes about is the same as that of the change result.

2.2. Directing consolidated plan

In these plans, each source hub partitions the first information into a few sections and transmits them in multi-way, while the middle of the road hubs makes some further procedure. In cut blend based plans [12], each source hub parts its unique information into a few cuts, and encodes them before sending them out in multipath. The moderate hub will unscramble these cuts and total them together. In secure system coding based plan [13], each source hub isolates the first information into a few squares what's more, dirties some of them. These squares are conveyed in multipath, what's more, will be re-encoded in the moderate hub. Each source hub additionally produces a few kinds of CRCs and encodes them. The security of square information is accomplished through the contamination component, which is in reality a sort of confusion system. Without unscrambling these CRCs, the foe is as yet conceivable to recuperation unique squares in the event that got enough bundles.

2.3. Destructive modification based scheme

In this kind of plan, the information protection is accomplished by applying a ruinous alteration on the first information. For instance, the information security of the differential protection based plan [7] is safeguarded by differential security hypothesis, where the arbitrary clamor is added to decrease the information certainty. The amusement hypothesis based plans [5,8] contemplate the entrance of private information by utilizing monetary approaches, for example, amusement hypothesis and contract hypothesis. Each source decides its security level and changes its information in view of the harmony thought of security and reward. Information gathered by these systems is regularly utilized for promote information mining.

2.4. Routing Schemes

Prasad et.al [16] presented different routing techniques in the IoT. An attack model is used for routing because of security issues in the IoT. Some of the attacks re-route the packets to the attacker’s controller. Through this information, the routing communication is extracted. Most common attacks are DDoS, Traffic hijacking, which exploits routing mechanism. Paul et.al [17] presented a multi hop protocol which uses multiple parameters for secure routing which have particular information already known as predefined for users. Resources are stored as routing information. Results are showed that secure multi-hop routing mechanism had been used for IoT communication.

Saleem et.al [15] proposed a bio-inspired secure IPv6 communication protocol for IoT. They enhanced the lossy network and low power transmission by classification algorithm called artificial immune system which classifies the misbehaving nodes and normal nodes with local information. Through the classification detection of excessive broadcast, improvements in power and transmission rate are increased. Results proved that transmission rate and energy consumption is far better than previously state of art routing techniques of IoT.

Liu et.al [14] proposed a SDN based IoT secure routing protocol. The issue in these IoT routing mechanism with SDN is security middlebox guard. SDN security based data transfer security model is reducing network latency and manage to secure data flow with the help of heuristic algorithms. Middle boxes with secure policies are placed at different locations. Next to tackle against changing of middleboxes to honeypot. They use offline integer program and also it is used to load balance. Experiments are demonstrated that this model can handle secure routing mechanism for IoT.

3. PROPOSED ENCRYPTION SCHEME

Compressive detecting based encryption scheme is basically an asymmetric encryption scheme. Figure 1 shows the architecture of the proposed encryption scheme. As per the matter of the fact, asymmetric encryption schemes are costlier for WSN applications when compared to other encryption schemes. However, these schemes can be made into minimalistic and can be deployed in sensor applications for better security. This can be achieved by limiting the security parameter sizes. Choosing the number of security parameters can also make the schemes feasible for deployment. This happens at the expense of the security of the scheme, but it was found that it still provides an appropriate level of security.

In the proposed encryption scheme, the public parameters chosen are a larger positive integer g which is 10^{200} and a positive integer d which is greater than two, as per the assumption. Hence the integer g should always have many small divisors and also many integers which are small when it is inverted modulo g. Consider, the following case for validation.

1. The first case proposed is that d should not be greater than 4 and should include the lower bound 2.
2. The second case is that g should not be greater than 2^{32}.

The list of parameters are always a positive integer r ∈ Zg and a positive integer g` which include $\log_g$, g is a always a secret security parameter. Finally, the secret key of the scheme is defined as (r, g`). Hence to encrypt the data from the WSN, $m \in Z_{g`}$, where d is always a random number (S_1 to S_d) should be generated $m = \sum_{j=1}^{d} s_j \ mod \ g'$ and $s_j > Z_g$. Further, the cipher text is then found as $E(m) = \sum_{j=1}^{d} s_j \ mod \ g'$. Additionally, addition and subtraction are to be done component wise where multiplication and division is done by multiplying the components of Z_g.

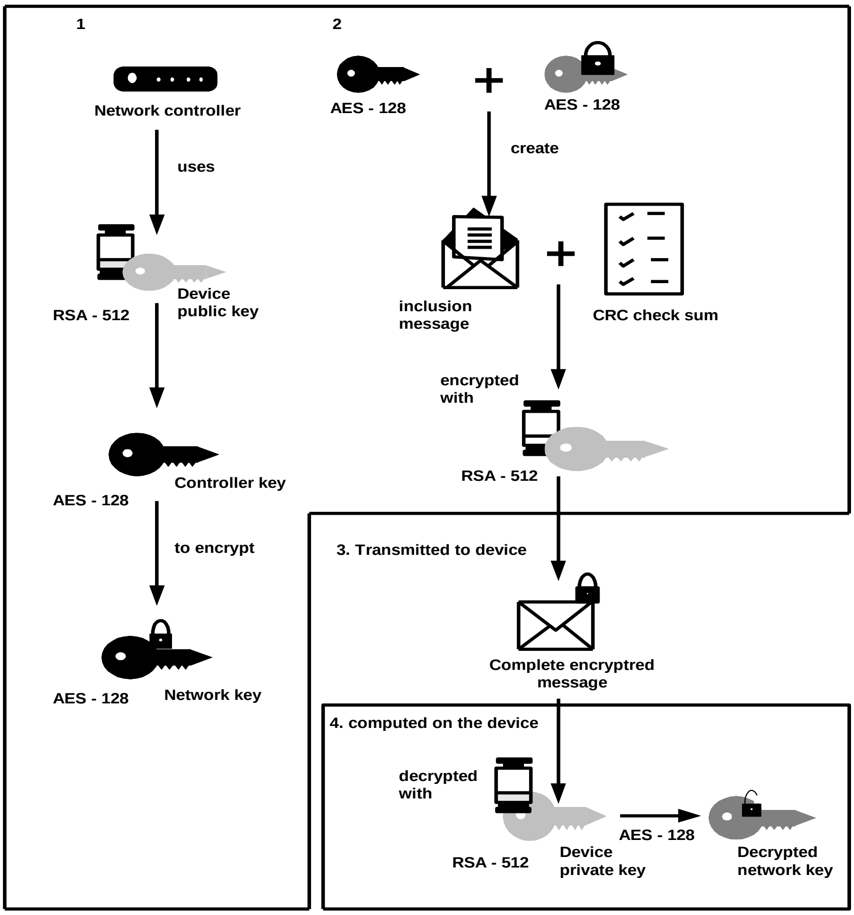

Figure 1. Architecture of the Proposed Crypto-System for WSN

4. EXPERIMENTAL SETUP

The proposed encryption scheme is implemented on Node Red and the nodes are deployed independently to monitor the water tank which contains shrimps. Each node is executed to run encryption scheme in order to ensure that each node communication is encrypted. A checksum is created and certificate pinning is also ensured in all nodes in order to verify the authenticity of nodes and to avoid the node cloning activities. The entire scheme is implemented using python. Figure 2 shows the architecture of sensor. Table 1 shows the data aggregation rate for various size of network.

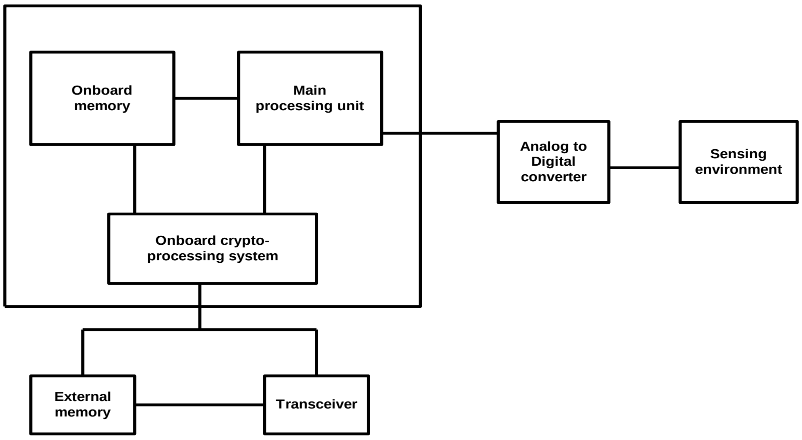

Figure 2. Architecture of the Sensor Deployment

Table 1. Encrypted Traffic Analyzed for Various Iteration with Increased Number of Nodes

25 nodes								
	Plain text		Round 1		Round 2		Round 3	
Node	Trans	Receiv	Trans	Receiv	Trans	Receiv	Trans	Receiv
1	50	20	110	70	120	75	131	70
2	52	30	120	80	134	82	151	98
3	54	34	134	90	140	94	166	110
4	60	45	154	110	160	125	172	120
50 nodes								
	Plain text		Round 1		Round 2		Round 3	
Node	Trans	Receiv	Trans	Receiv	Trans	Receiv	Trans	Receiv
1	70	30	140	80	150	87	151	80
2	72	40	150	99	164	110	167	112
3	74	54	164	119	170	123	178	132
4	80	65	184	140	180	190	197	145
75 nodes								
	Plain text		Round 1		Round 2		Round 3	
Node	Trans	Receiv	Trans	Receiv	Trans	Receiv	Trans	Receiv
1	80	40	156	99	166	90	165	100
2	97	55	167	112	176	112	176	123
3	99	67	187	123	187	132	187	154
4	110	76	198	154	199	212	210	198

4.1. Performance Analysis

The following parameters are selected for evaluation of the proposed asymmetric encryption algorithms for both encryption and decryption schemes.

1. Encryption Time
   The encryption time is considered as the time that an encryption algorithm takes to produces a ciphertext from a plain text. Fig. 4 and Fig. 6 shows the encryption time of various file size.
2. Decryption Time
   The decryption time is considered as the time that a decryption algorithm takes to reproduces a plain text from a ciphertext. Figure 3 and Figure 5 shows the decryption time of various file size.
3. Throughput
   Throughput is equal to total plaintext in bytes encrypted divided by the encryption time. Higher the throughput, higher will be the performance.
4. Encrypted File Size
   The size of encrypted file is called encrypted file size.
5. Decrypted File Size
   The size of decrypted file is called decrypted file size.

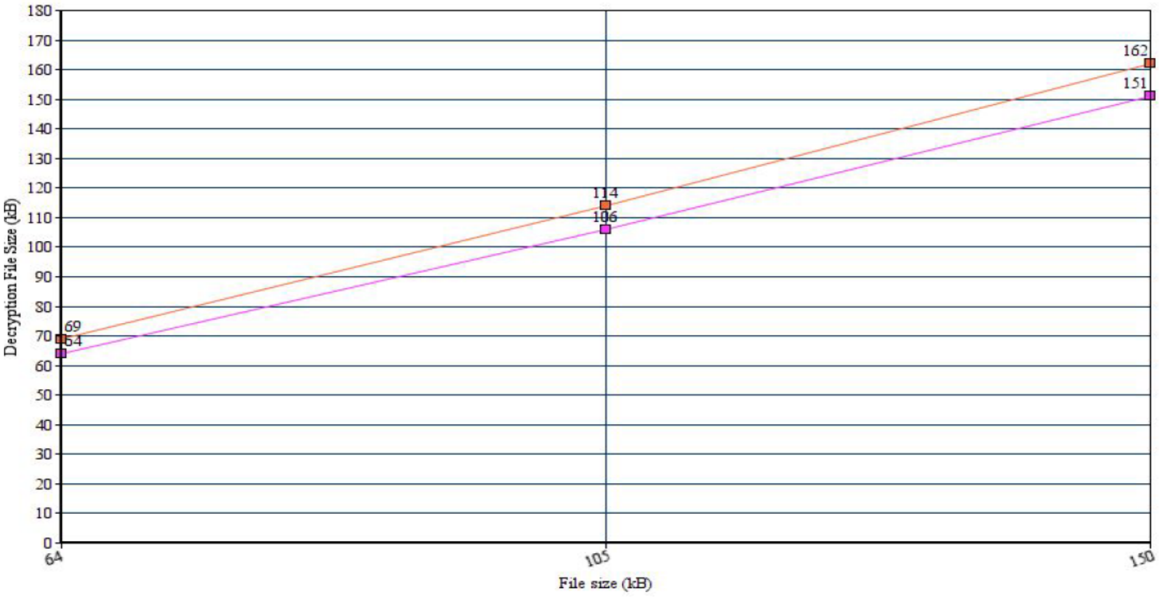

Figure 3. Decryption File Size (Proposed Homomorphic Scheme vs Existing Homomorphic Scheme)

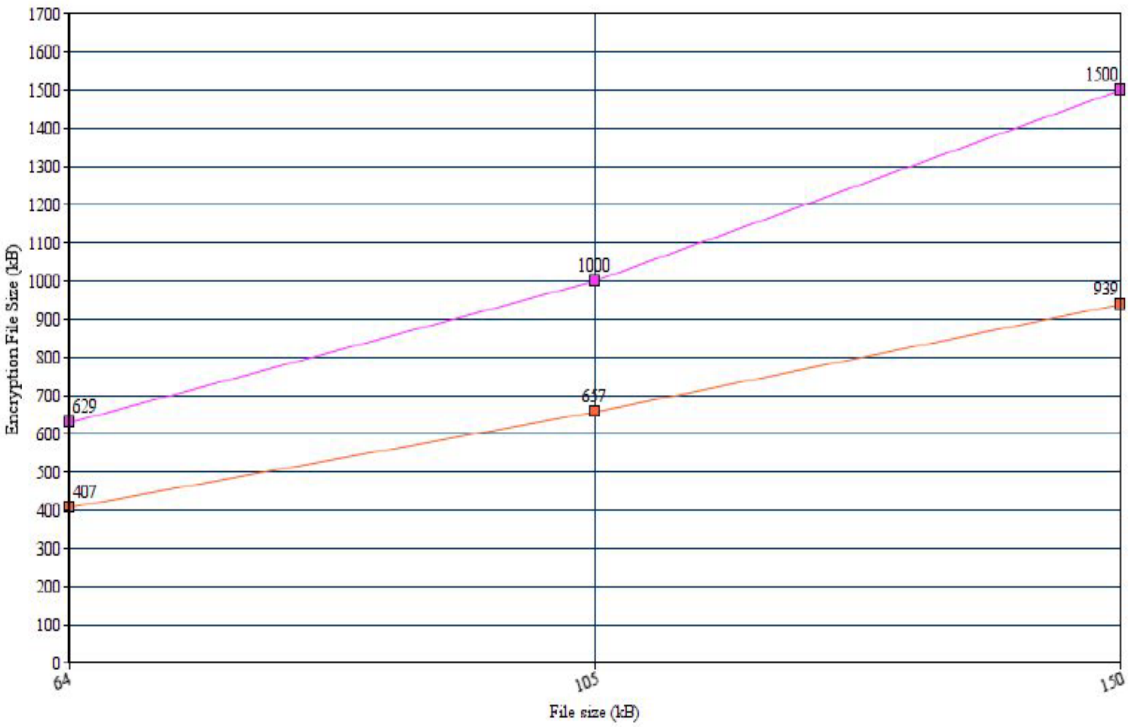

Figure 4. Encryption File Size (Proposed Homomorphic Scheme vs Existing Homomorphic Scheme)

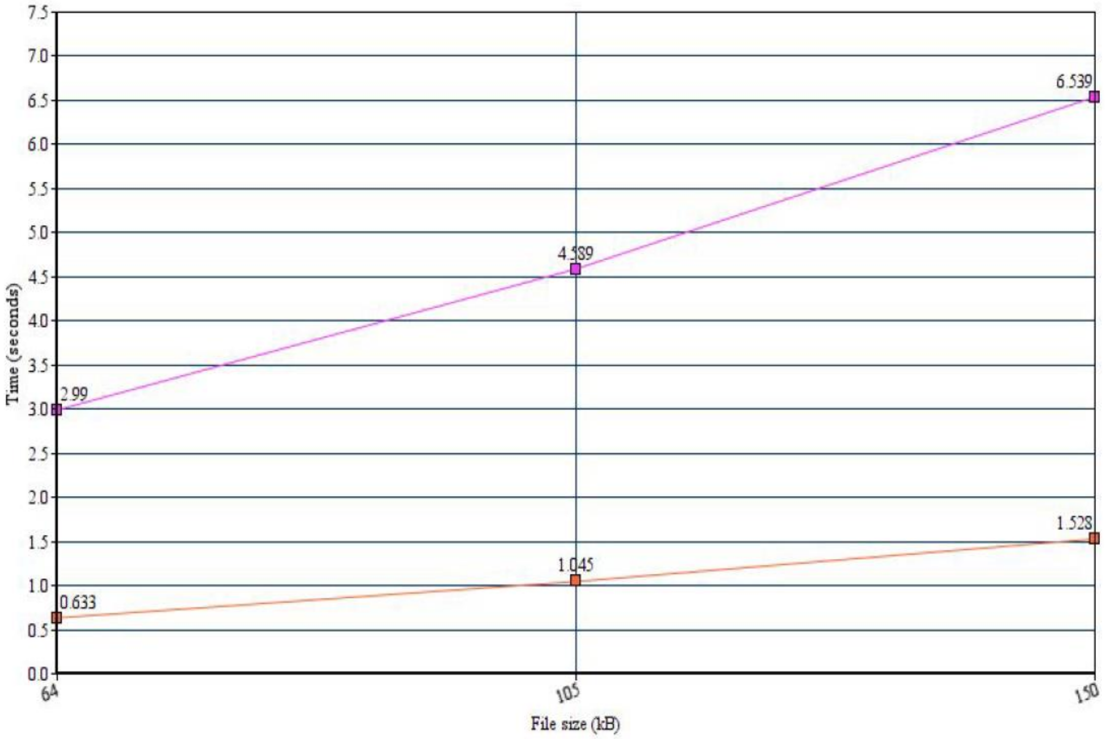

Figure 5. Decryption Time (Proposed Homomorphic Scheme vs Existing Homomorphic Scheme)

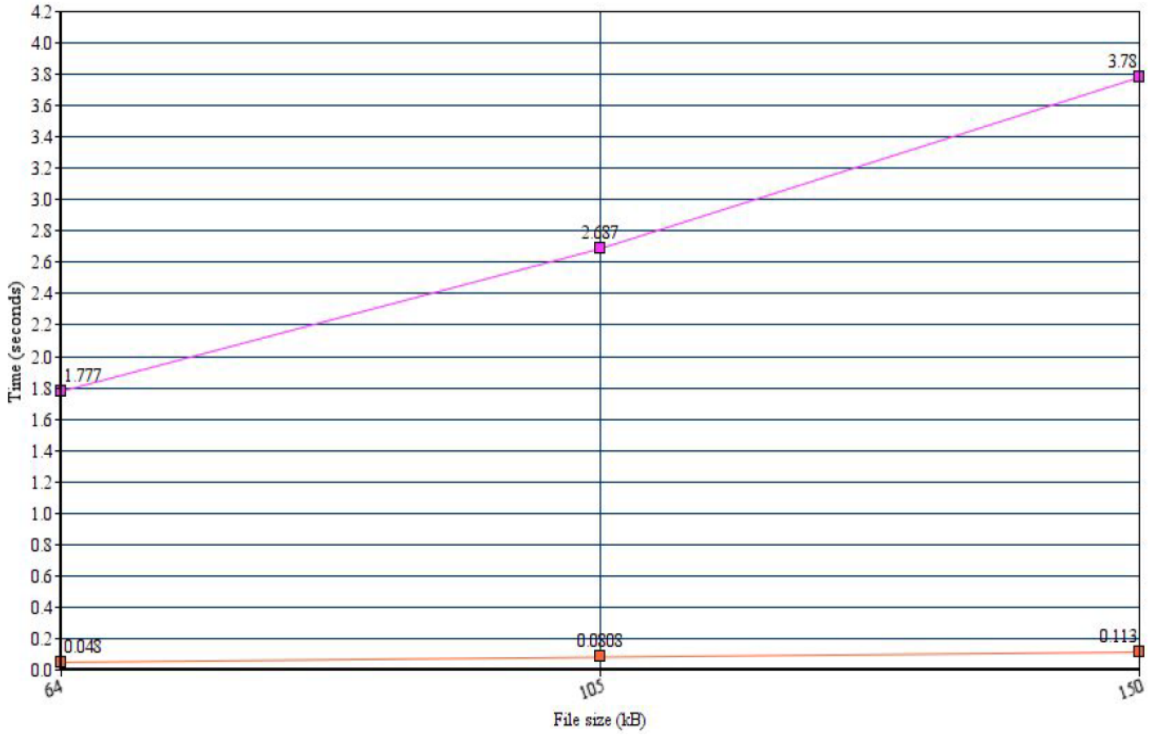

Figure 6. Encryption Time (Proposed Homomorphic Scheme vs Existing Homomorphic Scheme)

5. CONCLUSION

WSN is popular in increasingly gaining popularity in most of the applications in various domains. In order to provide security to the sensor node communication, this paper presented a homomorphic encryption scheme which allows data processing on a node encryption. Further it is also found that the proposed encryption scheme is for all sorts of networks. Even if the network size grows, the proposed scheme is capable to work on. It was also found that the proposed encryption scheme does not significantly reduce the performance of plaintext aggregation. This means that the proposed encryption scheme is feasible for WSN applications while considering its effect on network traffic.

REFERENCES

[1] J. H. Cheon *et al*., "Toward a Secure Drone System: Flying with Real-Time Homomorphic Authenticated Encryption", In *IEEE Access*, vol. 6, pp. 24325-24339, 2018.

[2] H. Chen, Y. Hu and Z. Lian, "Leveled Homomorphic Encryption in Certificateless Cryptosystem", In *Chinese Journal of Electronics*, vol. 26, no. 6, pp. 1213-1220, 2017.

[3] H. Chen, Y. Hu and Z. Lian, "Properties of SV-Style Homomorphic Encryption and Their Application", In *Chinese Journal of Electronics*, vol. 26, no. 5, pp. 926-932, 2017.

[4] B. Wang, Y. Zhan and Z. Zhang, "Cryptanalysis of a Symmetric Fully Homomorphic Encryption Scheme", In *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 6, pp. 1460-1467, June 2018.

[5] L. T. Phong, Y. Aono, T. Hayashi, L. Wang and S. Moriai, "Privacy-Preserving Deep Learning via Additively Homomorphic Encryption", In *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 5, pp. 1333-1345, May 2018.

[6] Alabdulatif, H. Kumarage, I. Khalil, M. Atiquzzaman and X. Yi, "Privacy-preserving cloud-based billing with lightweight homomorphic encryption for sensor-enabled smart grid infrastructure", In *IET Wireless Sensor Systems*, vol. 7, no. 6, pp. 182-190, 12 2017.

[7] L. Chen, M. Lim and Z. Fan, "A Public Key Compression Scheme for Fully Homomorphic Encryption Based on Quadratic Parameters With Correction", In *IEEE Access*, vol. 5, pp. 17692-17700, 2017.

[8] K. Lauter, "Postquantum Opportunities: Lattices, Homomorphic Encryption, and Supersingular Isogeny Graphs", In *IEEE Security & Privacy*, vol. 15, no. 4, pp. 22-27, 2017.

[9] Y. Ma, L. Wu, X. Gu, J. He and Z. Yang, "A Secure Face-Verification Scheme Based on Homomorphic Encryption and Deep Neural Networks", In *IEEE Access*, vol. 5, pp. 16532-16538, 2017.

[10] N. Dowlin, R. Gilad-Bachrach, K. Laine, K. Lauter, M. Naehrig and J. Wernsing, "Manual for Using Homomorphic Encryption for Bioinformatics", In *Proceedings of the IEEE*, vol. 105, no. 3, pp. 552-567, March 2017.

[11] Khedr and G. Gulak, “SecureMed: Secure Medical Computation Using GPU-Accelerated Homomorphic Encryption Scheme”, In *IEEE Journal of Biomedical and Health Informatics*, vol. 22, no. 2, pp. 597-606, March 2018.

[12] M. S. Lee, “Sparse subset sum problem from Gentry–Halevi's fully homomorphic encryption”, In *IET Information Security*, vol. 11, no. 1, pp. 34-37, 2017.

[13] R. Bocu and C. Costache, “A homomorphic encryption-based system for securely managing personal health metrics data”, In *IBM Journal of Research and Development*, vol. 62, no. 1, pp. 1:1-1:10, Jan.-Feb. 1 2018.

[14] Y. Liu, Y. Kuang, Y. Xiao and G. Xu, “SDN-Based Data Transfer Security for Internet of Things”, In *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 257-268, Feb. 2018.

[15] K. Saleem, J. Chaudhry, M. A. Orgun and J. Al-Muhtadi, “A bio-inspired secure IPv6 communication protocol for Internet of Things”, 2017 Eleventh International Conference on Sensing Technology (ICST), pp. 1-6, Sydney, NSW, 2017.

[16] Prasad, Shyam Sundar, and Chanakya Kumar, “An energy efficient and reliable internet of things”, In *Communication, Information & Computing Technology (ICCICT)*, pp. 1-4, IEEE, 2012.

[17] Paul AS Ward, Evan PC, Martin Karsten, and Jones, “Multipath load balancing in multi-hop wireless networks”, In *Wireless And Mobile Computing, Networking And Communications, (WiMob'2005),* IEEE International Conference, vol. 2, pp. 158-166, 2005.

BIOGRAPHIES OF AUTHORS

Dr.G.Ramachandran received the B.E degree in Computer Science and Engineering from Annamalai University in 1997. He received the M.E degree in Computer Science and Engineering from Annamalai University in the year 2005. He has been with Annamalai University, since 2000. He completed his Ph.D degree in Computer Science and Engineering at Annamalai University, in the year 2014. He published 30 papers in International conferences and Journals. His research interest includes Computer Networks, Network Security, Wireless Networks, Mobile Ad hoc networks and IoT.

S. Nagavalli received the B.Sc degree in Computer Science from CKN college in 2002. She completed her M.C.A degree from AVC college in the year 2005. She received her M.Phil degree from Annamalai University in 2008. She is doing her Ph.D degree in Department of Computer and Information Science at Annamalai University. She has published 3 papers in International Journals. Her area of interest includes Internet of Things, Cryptography, and Computer Networks.