Journal of trends in Computer Science and Smart technology (TCSST) (2020)
Vol.02/ No. 02
Pages: 98-108
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2020.2.004

Novel Shared Key Transfer Protocol for Secure Data Transmission in Distributed Wireless Networks

Dr. Akey Sungheetha
Data Science SIG member,
Computer Science and Engineering, School of Electrical Engineering and Computing,
Adama Science and Technology University, Adama, Nazret, Ethiopia

Dr. Rajesh Sharma R
Image Processing SIG member,
Computer Science and Engineering, School of Electrical Engineering and Computing,
Adama Science and Technology University, Adama, Nazret, Ethiopia

Abstract: Handling Keys in the distributed wireless network is one of the most popular options that ensures the protection of data that are transmitted under various circumstances. It even assists the setting up, reversal and the looking after of keys across diverse. So this makes it requisite to process and produce a corporate key that is secret and as well as distribute it across the network that is decentralized. This sort of key is termed as the shared key. The shared key aids in the procedures of encrypting and decrypting the information's that are to be transmitted. Multitudes of applications are developed based on the decentralized wireless network such as wireless adhoc network, mobile adhoc networks, wireless sensor networks etc. are suggested with the secret key protection to enhance the security level while transmitting data. The shared key transfer protocol (SKTP) procedure accomplishes encryption /decryption for the message to be transferred it uses a group of key and shares them across a several transmissions that takes place across the head of the cluster and the nodes in the clustered paradigm. This shared collection of keys allows the consumer to encode and decode the message that is to be conveyed for all the consumers in a group enabling a member in the cluster to work together with the other member in the group around the data discovery. So the paper aims in establishing a novel shared key transfer protocol (N-SKTP) that is dynamic in nature and practically possible to secure the information transfer across the devices in the distributed wireless network. The N-SKTP utilizes the pubic key cryptography to develop a shared key group (SKG) for the manifold transmission in the network. The investigation of the performance of the proposed protocol using the network simulator -2 experimentally demonstrates the proficiency of the N-SKTP in the distributed wireless networks with limited resources.

Keywords: Distributed Wireless Networks, Secret Keys, N-SKTP, SKG, Encryption Decryption

ISSN: 2582-4104

Journal of trends in Computer Science and Smart technology (TCSST) (2020)
Vol.02/ No. 02
Pages: 98-108
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2020.2.004

1. Introduction

Usage of secret keys in communicating the information's between two points ensures the secureness of the data in the diverse communicating circumstances. The managing process for the secret keys takes care of the setting up, reversal and the looking after of secret keys across multitudes of working to-gather consumers. So this makes it requisite to process and produce a corporate key that is secret and as well as distribute it across the network that is decentralized. This sort of key is termed as the shared key. The shared key aids in the procedures of encrypting and decrypting the information's that are to be transmitted. Multitudes of applications are developed based on the decentralized wireless network such as wireless adhoc network, mobile adhoc networks, wireless sensor networks etc. are suggested with the secret key management (SKM) to enhance the security level while transmitting data.

The decentralized networks in form wireless adhoc networks formed using homogenous devices or heterogeneous devices or using the sensor nodes is a malleable organization that are capable of firming up the on the horizon applications group. To facilitate the protection for specific chores allowing them have their privacy. It becomes requisite to accomplish a shared key for the purpose of encrypting the data across the group of associates in a network. As the distributed network based on the sensor nodes are often deployed in unreceptive environments, choosing management of keys with the dynamic property is essential. Nonetheless the listed reasons complicate the security measures in the distributed wireless networks they are

i. Dynamic Topology
ii. Decentralized infrastructure
iii clubbing and segregating of clusters in the paradigm
iv. Repeated connection failures

Based on the above mentioned reasons the numerous management schemes for maintaining the keys were developed for the adhoc networks. Relying on the diverse factors the prevailing developments were distinguished as "static key management design and the dynamic key management design" in the existing static methods the key remained static for a longer duration, while in dynamic the keys were refreshed periodically.

ISSN: 2582-4104

Journal of trends in Computer Science and Smart technology (TCSST) (2020)
Vol.02/ No. 02
Pages: 98-108
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2020.2.004

To establish a security imposed transmission across the sensor nodes deployed in a decentralized manner. Either a pair off or the SKG protocols to manage the keys are used. The figure.1 below shows four different types of schemes in managing the keys.

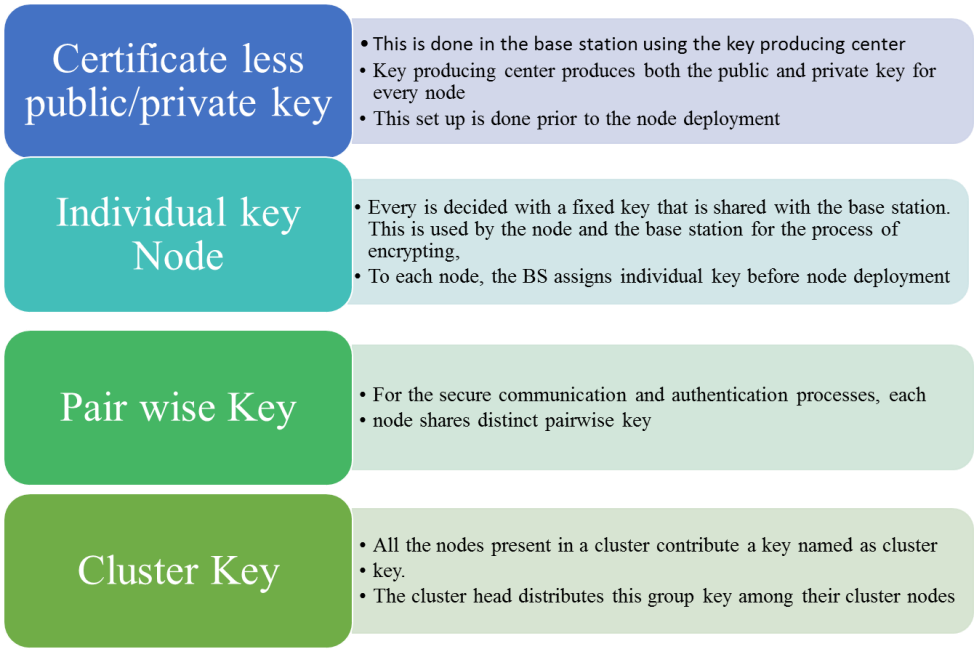

Figure.1 Key Managing Schemes

So to deliver a secured and protected data transmission for any sort of network. Management of keys takes a significant part. Apart from this processing and producing a secret code that is shared and dispersing them across the nodes/devices in the network is also prerequisite. Due to the dynamic topology developing and looking after a cluster has become a predominant area of research. The constructing clusters enables the refreshing the keys without difficulties.

The paper is about the modest as well as proficient protection measures strategies that concentrates on the cluster communication in the devices connected in the distributed manner. The key contributions of the paper are.

ISSN: 2582-4104

Journal of trends in Computer Science and Smart technology (TCSST) (2020)
Vol.02/ No. 02
Pages: 98-108
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2020.2.004

- An N-SKTP with dynamic managing attributes to afford security for the data transmission in the distributed networks
- Examination of secureness and the complexity endured by the proposed method employing the network simulator-II

The proposed encryption/decryption strategy is hold out with the related work in two the proposed work in three the results evaluation in four and the conclusion in five.

2. Related Works

The part provides the particulars of the different strategies that emerged in the past decades, the DH centered "Chinese remainder theorem" was proposed by the author Balachandran et al [1] to offer a communication with cluster of keys. In Zhu et al [2] a strategy following a probabilistic methodology for the managing the cluster key was presented. A dual-round key handling protocol was devised by the author Rahman, et al [3]. Mukherjee et al [4] has presented the "distributed key management procedure" that is centered on the " threshold cryptography" to ensure the secureness of the information's that are transmitted among the decentralized network.

Li, et al [5] proposes a method to "segregate the clusters into to small divisions and secure the transmission using the dual party DU agreement protocol" and Cho et al [6] devises an "cluster based group key management protocol" Drira, et al [7] recommended the SKG structures that incorporated "trust based cryptographic methods" to preserve the privacy of the data transmitted. Bellazreg et al [8] proposed a" dynamic tunneling and group key management" for securing the information transfer among the collective associates. Yang, et al [9] put forth a capacity to construct the SKG with the innovative cluster keys and the consumers or while the prevailing member leaves with the help of "LSSS an ElGammal" cryptography.

The authors Praveena, A., and S. Smys et al [10] put forth an "Efficient cryptographic approach for data security in wireless sensor networks using MES VU." Suma, V. et al [11] performed the "Security and Privacy Mechanism Using Blockchain"

Sridhar, S., et al [12] framed a "Intelligent security framework for iot devices cryptography based end-to-end security architecture." Mugunthan, S. R et al [13] devised a "Security and Privacy Preserving of Sensor Data Localization Based on Internet of Things" Kumar, Dinesh, Set al [14] performed the "Fault Detection Methodology in Wireless Sensor Network."

ISSN: 2582-4104

Journal of trends in Computer Science and Smart technology (TCSST) (2020)
Vol.02/ No. 02
Pages: 98-108
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2020.2.004

3. Novel Shared Key Transfer Protocol

The N-SKTP is framed with dual protocols, on for the purpose of transferring and the other for the purpose of agreement. The figure.2 below depicts basic network model with the clustering environment and the SKG establishment.

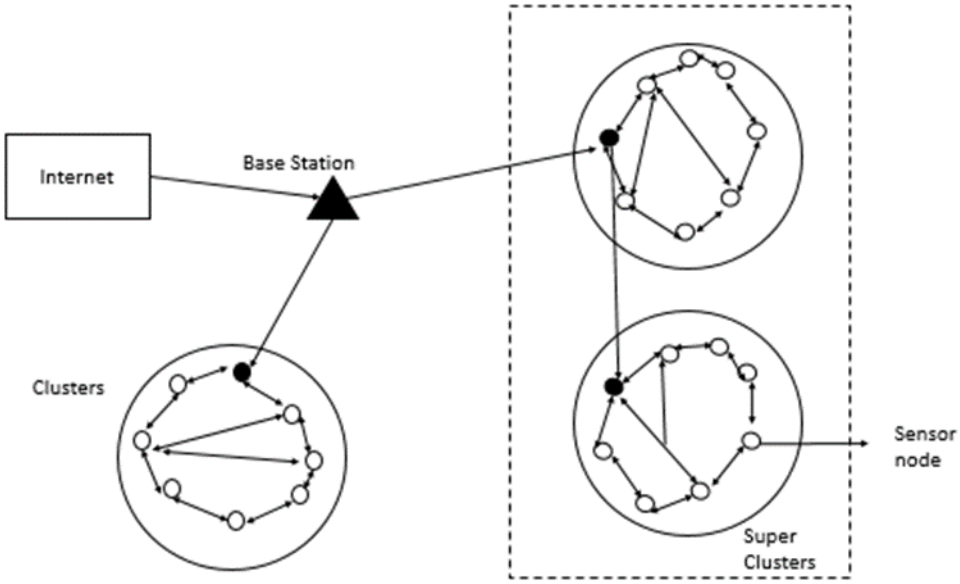

Figure.2 Basic Network Model with Clusters and SKG

The transfer protocol depend on a confidential unit for the production of the secret keys. The algorithm below depicts the process involved.

- For a network of size 'i' the SKG is segregated into 'i' parts and is dispersed among the 'i' nodes such that the number of the parts segregate's' is equal or lesser than the SKG. This condition makes the construction of the actual secret possible otherwise the reconstruction becomes difficult.
- The head in the cluster chooses the polynomial "$f(x) = a0(x) + a2\ (x^2)$ ... ... $+ a(t-1)(x^t - 1)$" where $a(t-1)$ is a "degree polynomial". While SKG = a0= f(0) and all the other factors a0, a1,… are present in a "finite field" FF(n) = Group FF(n) with 'n' elements.

ISSN: 2582-4104

Journal of trends in Computer Science and Smart technology (TCSST) (2020)
Vol.02/ No. 02
Pages: 98-108
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2020.2.004

- The head estimates the $key(x) = f(x) mod n$ where 'x'= 1….i
- The head projects the list of outputs of 'i' parts $(k1, k2 \ldots . ki)$ for every i_x
- Every node is now capable of reconstructing the SKG using "Group-Key" = $f(0) = \sum_{x \in c} k_x \prod_{j \in c-x} \left(\frac{y_j}{y_j - y_x}\right) mod\ n$

The agreement protocols for the SKG is developed using the DH cryptographic method followed in [1]

The SKG establishment using the N-SKTP in the clustered environment initiates by organizing the network into clusters. Every cluster is framed with a head and the members. The SKG procedure is processed into the clusters to accomplish a SKG across the head and the members. The figure .3 below is shows the phases in the SKG generation using the N-SKTP.

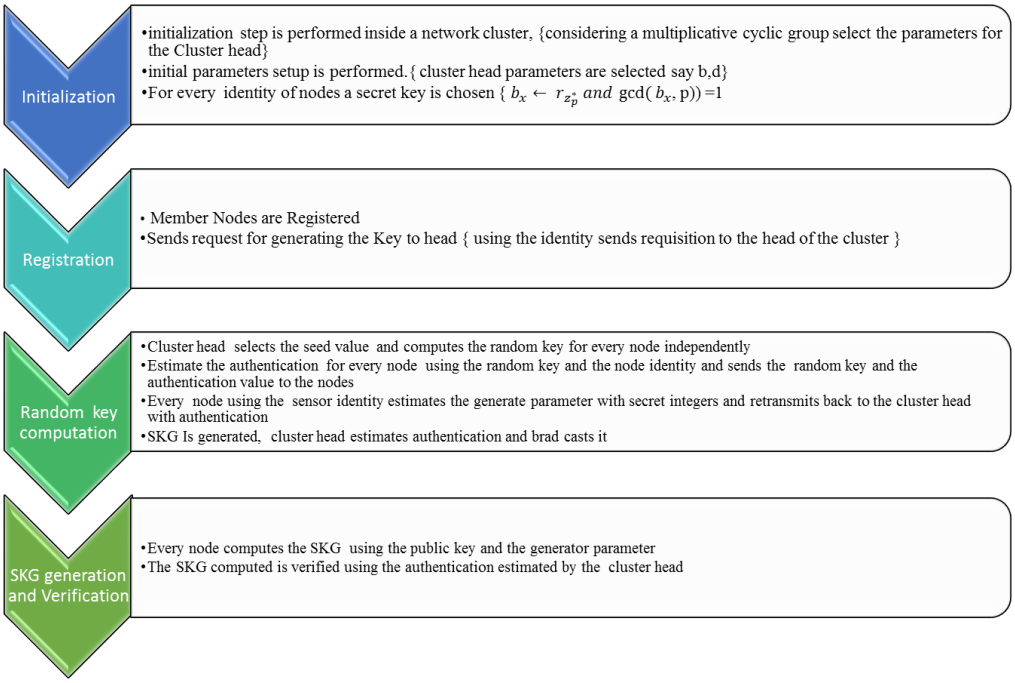

Figure.3 Proposed Protocol

ISSN: 2582-4104

Journal of trends in Computer Science and Smart technology (TCSST) (2020)
Vol.02/ No. 02
Pages: 98-108
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2020.2.004

4. Results Evaluation

An open source "discrete event driven" simulator is utilized to simulate the proposed protocol. Two different network arrangement star and internet are selected for the experimental validation of the proposed approach. The table.1 below lists down the necessary parameters used in the simulation process.

S.No	Parameter	Value
1	Channel type	wireless
2	Routing protocol	AODV
3	Length of queue	50
4	No. of Nodes	80
5	Node deployment	Random
6	Simulation End Time	100seconds
7	Packet Size	1024bytes
8	Path loss model	Two-ray ground
9	Energy	1000 joules
10	Communication range	500mx500m

Tabel.1 Parameters and the Configuration used

The simulation process examines the management of the key generated utilizing various parametric such as "bandwidth for the throughput and the network traffic". The samples were collected by the simulator to sample the traffic including the total level of traffic in the network. The experiment and the sample collection for conducted at regular time intervals.

ISSN: 2582-4104

Journal of trends in Computer Science and Smart technology (TCSST) (2020)
Vol.02/ No. 02
Pages: 98-108
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2020.2.004

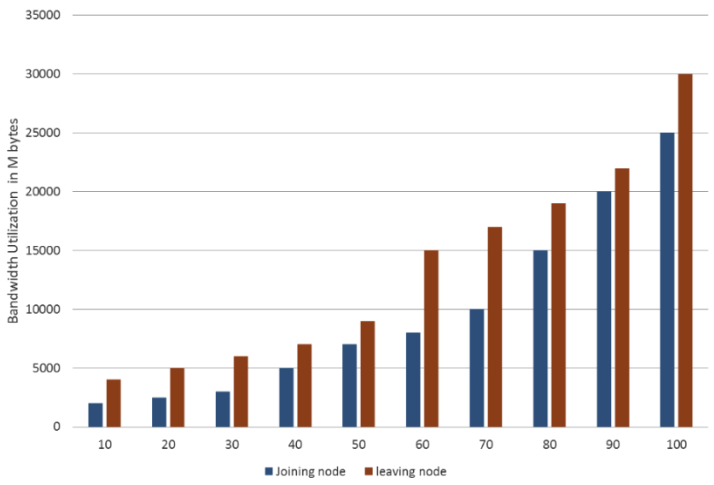

Figure.4 Bandwidth Utilization

The figure.4 shows the bandwidth utilization while a node parts and joins the network is observed over a regular periods and the figure.5 below provides the percentage of network traffic while new nodes are joined in the network, on initializing the N-SKTP in the distributed wireless networks

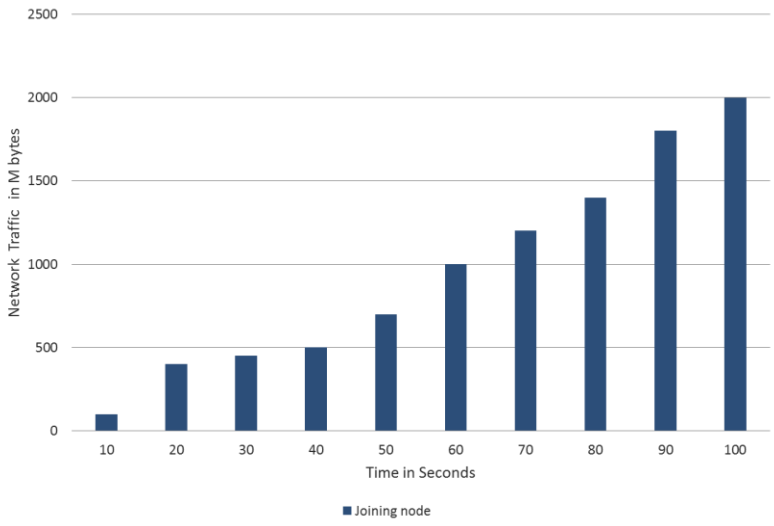

Figure.5 Network Traffic

ISSN: 2582-4104

Journal of trends in Computer Science and Smart technology (TCSST) (2020)
Vol.02/ No. 02
Pages: 98-108
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2020.2.004

The percentage of throughput and the percentage of delay observed in network on using the N-SKTP is observed below in the figure.6

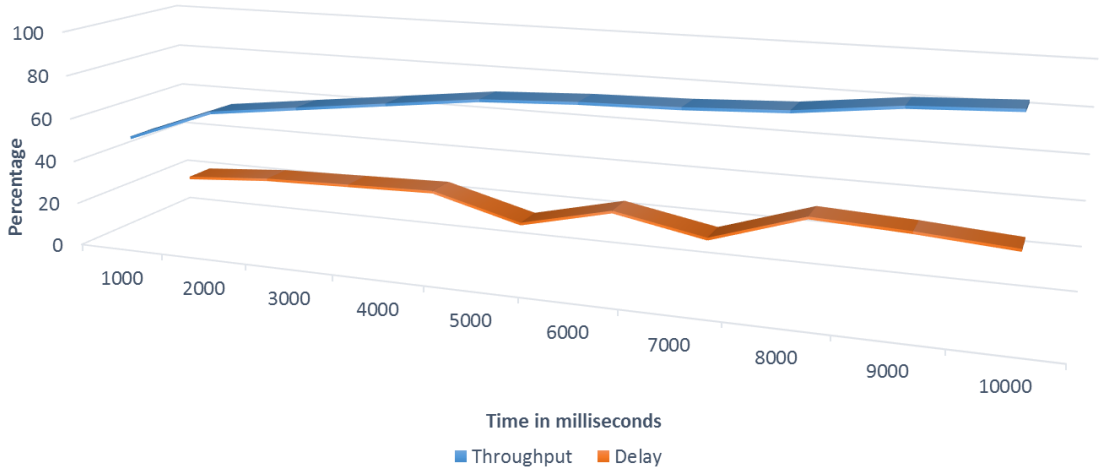

Figure.6 Throughput and Delay

The results obtained shows that the setting the N-SKTP in the wireless network that is distributed has not affected the throughput of the packet transmission and in fact has improved the data transmission rate as the data are properly delivered to its authenticated consumers and the percentage of delay seems to be normal delay incurred in transmission including the processing, route discovery, route establishment, transmission etc. Through the experiment conducted over the wireless medium using the MAC protocol IEEE 802.11 to authenticate with a CBR traffic type has evinced the proficiency of the proposed method.

5. Conclusion

The decentralized networks in form wireless adhoc networks formed using homogenous devices or heterogeneous devices or using the sensor nodes is a malleable organization that are capable of firming up the on the horizon applications group. To facilitate the protection for specific chores allowing them have their privacy. It becomes requisite to accomplish a shared key for the purpose of encrypting the data across the group of associates in a network. As the distributed network based on the sensor nodes are often deployed in unreceptive environments, choosing management of keys with the dynamic property is

ISSN: 2582-4104

essential. So to enhance the security in the distributed network the proposed method has put forth an N-SKTP with the capability of verification. The analysis performed using the NS-II evinces the competency of the proposed method.

References

[1] Balachandran, Ravi K., Byrav Ramamurthy, Xukai Zou, and N. Variyam Vinodchandran. "CRTDH: an efficient key agreement scheme for secure group communications in wireless ad hoc networks." In *IEEE International Conference on Communications, 2005. ICC 2005. 2005*, vol. 2, pp. 1123-1127. IEEE, 2005.

[2] Zhu, Sencun, Sanjeev Setia, Shouhuai Xu, and Sushil Jajodia. "GKMPAN: An efficient group rekeying scheme for secure multicast in ad-hoc networks." *Journal of Computer Security* 14, no. 4 (2006): 301-325.

[3] Rahman, Rony Hasinur, and M. Lutfar Rahman. "An efficient group key agreement protocol for ad-hoc networks." In *2008 International Conference on Electrical and Computer Engineering*, pp. 478-483. IEEE, 2008.

[4] Mukherjee, Anindo, Anurag Gupta, and Dharma P. Agrawal. "Distributed key management for dynamic groups in MANETs." *Pervasive and Mobile Computing* 4, no. 4 (2008): 562-578.

[5] Li, Xiang-Yang, Yu Wang, and Ophir Frieder. "Efficient hybrid key agreement protocol for wireless ad hoc networks." In *Proceedings. Eleventh International Conference on Computer Communications and Networks*, pp. 404-409. IEEE, 2002.

[6] Cho, Jin-Hee, Ray Chen, and Ding-Chau Wang. "Performance optimization of region-based group key management in mobile ad hoc networks." *Performance Evaluation* 65, no. 5 (2008): 319-344.

[7] Drira, Kaouther, Hamida Seba, and Hamamache Kheddouci. "ECGK: An efficient clustering scheme for group key management in MANETs." *Computer Communications* 33, no. 9 (2010): 1094-1107.

[8] Bellazreg, Ramzi, and Noureddine Boudriga. "DynTunKey: a dynamic distributed group key tunneling management protocol for heterogeneous wireless sensor networks." *EURASIP Journal on Wireless Communications and Networking* 2014, no. 1 (2014): 9.

[9] Yang, Yang, Yupu Hu, Chun-hui Sun, Chao Lv, and Leyou Zhang. "An efficient group key agreement scheme for mobile ad-hoc networks." *Int. Arab J. Inf. Technol.* 10, no. 1 (2013): 10-17.

[10] Praveena, A., and S. Smys. "Efficient cryptographic approach for data security in wireless sensor networks using MES VU." In 2016 10th international conference on intelligent systems and control (ISCO), pp. 1-6. IEEE, 2016.

ISSN: 2582-4104

[11] Suma, V. (2019). Security and Privacy Mechanism Using Blockchain. Journal of Ubiquitous Computing and Communication Technologies (UCCT), 1(01), 45-54.

[12] Sridhar, S., and S. Smys. "Intelligent security framework for iot devices cryptography based end-to-end security architecture." In 2017 International Conference on Inventive Systems and Control (ICISC), pp. 1-5. IEEE, 2017

[13] . Mugunthan, S. R. (2019). Security And Privacy Preserving Of Sensor Data Localization Based On Internet Of Things. Journal of Ismac, 1(02) 81-92.

[14] Kumar, Dinesh, S. Smys, G. Smilarubavathy, and Frank Holzwarth. "Fault Detection Methodology in Wireless Sensor Network." In 2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), 2018 2nd International Conference on, pp. 723-728. IEEE, 2018.

Author's Biography

Dr. Akey Sungheetha is a Data Science SIG member, in the department of Computer Science and Engineering, in School of Electrical Engineering and Computing, in Adama Science and Technology University, Adama, Nazret, Ethiopia her major area of research includes Computer Networks, Chaos Theory, Particle Swarm Optimization, Probabilistic Computing, Fuzzy, Bio- Inspired Computing, Data Visualization, Fault Diagnosis.

Dr. Rajesh Sharma R is an Image Processing SIG member, in Computer Science and Engineering department, School of Electrical Engineering and Computing, Adama Science and Technology University, Adama, Nazret, Ethiopia his major area of research includes Wireless Communications, Cloud Computing, Computer System Engineering, Communication Technologies, Information Processing, Computer Networks, Web Technologies, Computing & Communications, Automation, Image processing

ISSN: 2582-4104