J. Appl. Math. & Informatics Vol. **41***(2023), No. 1, pp. 95 - 105*
https://doi.org/10.14317/jami.2023.095

GRID BASED ENERGY EFFICIENT AND SECURED DATA TRANSACTION FOR CLOUD ASSISTED WSN-IOT

L. SASIREGA*, C. SHANTHI

Abstract. To make the network energy efficient and to protect the network from malignant user's energy efficient grid based secret key sharing scheme is proposed. The cost function is evaluated to select the optimal nodes for carrying out the data transaction process. The network is split into equal number of grids and each grid is placed with certain number of nodes. The node cost function is estimated for all the nodes present in the network. Once the optimal energy proficient nodes are selected then the data transaction process is carried out in a secured way using malicious nodes filtration process. Therefore, the message is transmitted in a secret sharing method to the end user and this process makes the network more efficient. The proposed work is evaluated in network simulated and the performance of the work are analysed in terms of energy, delay, packet delivery ratio, and false detection ratio. From the result, we observed that the work outperforms the other works and achieves better energy and reduced packet rate.

AMS Mathematics Subject Classification : 65D30, 65D32.
Key words and phrases : Node cost computation, energy efficient, node reputation, cloud service provider, third party auditing, WSN-IoT.

1. Introduction

Wireless Sensor Networks (WSNs) is a self-organizing distributed sensor network consists of hundreds of tiny sensor nodes with sensing capabilities. In general the nodes are deployed randomly in difficult and terrible environments to perform various complex tasks [1]. The nodes that located outside of the network collect the broadcasted data and decide to join the network [2]. In various fields the wireless network is employed since it has the capability of processing and transmitting the data includes healthcare monitoring, smart city, battlefield surveillance, intrusion detection, emergency response Internet of Things (IoT)

Received February 3, 2022. Revised August 14, 2022. Accepted October 12, 2022.
*Corresponding author.

[3] etc. Lot of research work is in progress in IoT domain which helps for the overall development of the society and makes the lives easy and comfortable. But in the resource constrained environment of WSN and IoT, it is almost inconceivable to establish a fully secure system [4]. As we are moving forward very fast, technology is becoming more and more vulnerable to the security threats. The main objective of IoT security is to preserve privacy, confidentiality, ensure the security of the users, infrastructures, data, and devices of the IoT, and guarantee the availability of the services offered by an IoT ecosystem [5]. The network of physical objects such as vehicles, electronic devices, organizations and other things that are embedded with software, sensors and network connectivity that allows the things to communicate with each other by exchanging their data [6]. Therefore, the IoT has been widely applied in various applications and is the next major link in the new technology domain. IoT and Cloud Computing together with a focus on the security issues of both technologies was monitored [7]. Specifically, Cloud Computing and IoT are the aforementioned technologies here the common features are examined and the benefits of their integration was discovered. The rest of the work is structured as follows. Section 2 discusses the currently available solution for the security of WSN. Section 3 introduces the proposed work and discusses the process of the proposed work. Results obtained for the proposed work is discussed in section 4. Section 5 concludes the work

2. Related works

Some protocols based on energy efficient WSN and cloud's trustworthiness are discussed here for reference. Trust computation models are very effective to mitigate the internal attacks. A differential method for evaluation of direct trust was proposed in [8] which use the hysteresis curve for effective trust evaluation. Trust-based solutions have proved to be more effective for addressing the nodes' misbehavior attacks. Trust and Energy aware Routing Protocol (TERP) was proposed [9] that makes use of a distributed trust model for the detection and isolation of misbehaving and faulty nodes. Moreover, TERP incorporates a composite routing function that encompasses trust, residual-energy, and hop-counts of neighbor nodes in making routing decisions. This multi-facet routing strategy helps to balance out energy consumption among trusted nodes, while routing data using shorter paths. Beta and LQI-based Trust Model (BLTM) for the WSNs was proposed in [10]. Here initially, communication trust, energy trust, and data trust are considered when calculating direct trust. Then, the weight of communication trust, energy trust, and data trust are discussed. Connor, a novel graph encryption scheme that enables approximate Constrained Shortest Distance (CSD) querying was proposed [11]. Connor is built based on an efficient, tree-based ciphertext comparison protocol, and makes use of symmetric-key primitives and the somewhat homomorphic encryption, making it computationally efficient. Using Connor, a graph owner can first encrypt privacy-sensitive graphs and then outsource them to the cloud server, achieving the necessary privacy without losing the ability of querying. Lyapunov optimization theory and transform the formulated optimization problem into a queue stability problem, and further decompose the queue stability problem into two subproblems to solve the initial optimization problem. Therefore Stochastic Cost Minimization Mechanism (SCMM) consisting of two algorithms was proposed for solving the derived sub-problems [12]. The QoS-driven trust assessment method for cloud services is one of them. A compliance-based multi-dimensional trust evaluation system [13] was proposed to determine the trustworthiness of a Cloud Service Provider (CSP) by enabling cloud service provider. This system helps Cloud Service Centre (CSC) to choose a CSP from candidate CSPs that satisfy its desired QoS requirements. A trust-centric approach [14] based on hypergraph-binary fruit fly optimization was proposed for the identification of suitable and trustworthy CSPs. A trust assessment framework for the Security and Reputation of Cloud Services (SRCS) is proposed. This mechanism enables the trust evaluation of cloud services in order to ensure the security of the cloud-based IoT context via integrating security and reputation based trust assessment methods [15]. The security-based trust assessment method employs the cloud-specific security metrics to evaluate the security of a cloud service. Also the feedback ratings on the quality of cloud service are exploited in the reputation-based trust assessment method in order to evaluate the reputation of a cloud service. A trust evaluation method combined the feedback evaluation component and the Bayesian game model was proposed [16] to recognize malicious CSCs and their feedback ratings. The former is used to examine and identify fake identities and the latter is used to detect malicious users and their feedback. A trust evaluation method for collaborations of data-intensive services is considered in [17]. It considers not only the trust for individual partner services and the explicit trust relation among partner services that have logical dependencies for each other, but also the implicit trust relation implied in data-dependencies among services

3. GE2SDT - Proposed Method

Grid based Energy Efficient and Secured Data Transaction (GE2SDT) method is proposed. Here the network is divided into equal number of grids and each grid is placed with certain number of nodes for removing coverage connectivity issues. To find the energy efficient nodes in the grid the node cost function is estimated for all the nodes. Once the optimal energy proficient nodes are selected then the data transaction process is carried out in a secured way using malicious nodes filtration process. Figure 1 shows the system architecture of the proposed method. The node cost function is computed to determine the best grid lead nodes for data transaction from the sensing environment to the gateway or server

i. Node cost function estimation:

The node cost function is evaluated for each and every node in order to check

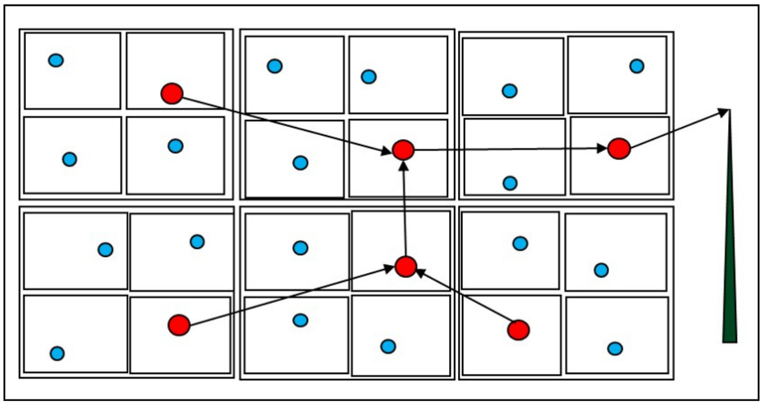

FIGURE 1. Dissimilar Data Extraction Methods in Healthcare

their optimality. The nodes that posses high node cost are considered to be optimal nodes. The estimation of node cost function includes node energy point and node reputation point. Therefore the optimal nodes are chosen by selecting the high energy and reputed point evaluated from the deployed nodes.

Selection of High Energy Nodes: Primary evaluation of node cost function is involved with energy computation. The energy computation is done for each node that present in the grids and the nodes with higher energy are selected for the data transaction purpose. This process can balance the energy level for the entire network process and prolongs the network lifetime. The energy level that is spent for the process of sensing, transmitting and receiving should be considered for the determination of remaining energy level of each node. The energy that is spent by the node for processing the data includes sensing (ES), transmitting (ET) and receiving (ER) and therefore SE is calculated using equation 1,

$$S_E = E_S + E_T + E_R \tag{1}$$

The remaining energy level (REL) can be calculated by taking the difference between the initial energy value (IE) and the spent energy value (SE). REL can be calculated using equation 2,

$$REL = ((I_E - S_E)/Time) \tag{2}$$

The threshold energy value is fixed and the nodes that have higher energy levels than the threshold is selected as higher energy level nodes than the reputation cost function is determined for the selected nodes.

Selection of Reputed Nodes: Secondary node cost function is determined through the computation of reputation of nodes. The reputed nodes are selected by evaluating the node processing quality. Node processing quality is computed through the ratio of number of request messages and the number of reply messages. The reputed threshold value is fixed and the node that holds higher value than the threshold value is selected as reputed nodes. Identifying the reputed nodes among the deployed nodes is mandate since the network may be compromised with malicious nodes and the information received from the malicious nodes can lead to mission failures. Therefore the selfish behaviour of the nodes is computed through the number of processing control messages with respect to the count. The node rank is computed through the success rate of processing of control messages. On basis of the node rank the reputation value for each node is computed and categorised into reputed nodes (RN) and malicious nodes (MN). Node rank computation is carried out by taking the ratio of processed reply messages with respect to the number of request message sent by the individual node and it is followed by equation 3.

$$N_R ank = \frac{NoofRREQprocessed_n}{NoofRREPprocessed_n}(75 > N_R > 100) \tag{3}$$

The average threshold for the reputed nodes is fixed between the values 75 and 100. The nodes that hold the rank between 75 and 100 is elected as reputed nodes. The certificate authority is given to each RN.

(ii) Cloud Level Data Integrity:

Nodes that are placed in the sensing environment process the real time data and transmit to the end user by utilizing the cloud computing mechanism. Though the data transaction is done through reputed nodes outsourced data confidentiality is still being a challenging one. Therefore data confidentiality through cloud level integrity is proposed here. The node cost function is determined and the information is collected through the reputed nodes which are then transacted to the cloud server. Malignant nodes cannot able to eavesdrop the outsourced data since the information is transacted through the reputed nodes to the server of the cloud. But cloud server is generally compromised of multiple divisions like private cloud, public cloud and hybrid cloud. The servers of private cloud belong to a single customer or company owned by a single owner. The data can be protected with high secured firewall. The third party providers cannot able to access the private cloud so easily since protected with security features. However the public cloud and the hybrid cloud service provider can be easily accessible by everyone as well as accessible by untrusted third party. Hence if the data confidentiality is not protected with strong security features then the perceptive or sensitive information will be disclosed to the malignant user. Without any data encryption process the sensed data is uploaded in the cloud server and the cloud server is considered to be untrusted, the confidentiality of the data might not be protected as well. Public auditing scheme of cloud assisted WSN-IoT is compromised of public cloud server, Sensor network, Client (user), Key generation centre and third-party auditor. In the cloud server the client can upload the sensed information to the cloud or download the sensed information from the cloud. The key generation centre is partially-trusted thing. The data integrity of the uploaded files or information and the received data from the sensor nodes is checked by the third party auditor (TA). Service provider (SP) analyses the user information and transacts the confidential information to the end user by verifying the TA auditions that involves True/False reports.

The partial private keys are generated by the key generation centre and given to the service provider (P—Pk). Each service provider is allotted with its own identity (Idi). The identity encryption is carried out with the partial public keys (Id(i)(SP)). The data transaction (D_{frame}, r_i) correctness is monitored and validated by the third party auditor and provides the information report with TRUE or FALSE statements along with the proof (P_r, D). TA executes the data integrity check for The service provider identity and its generated private key (P—Pk) are the preliminaries taken by the third party auditing. The data integrity 'Do' and/or 'Di' is computed by the TA and the resultant value 'R' is verified using the equation 4

$$D_0 = D(Id_(i)(SP), P|Pk_{SP}$$

$D_1 = D(Id_i, KD_frame), P|Pk_SP_1, P|Pk_SP_2$

$$R = \sum_{i}^{k} D_0 * D_i \tag{4}$$

The resultant value 'R' of the received data frame is checked and verified by the third party auditing and proves the data with the reports of TRUE and FALSE. The validating proof is given using equation 5,

$$e(P_r, D_frame) = e(D_i, D_frame + R.PK_SP1, D_0.D_frame \tag{5}$$

Thereby the validity certificate proofs along with the True and/or False reports are generated for each and every particular public service providers from which the end users can able to access the confidential information

4. Results and Discussion

The proposed scheme GE2SDT and the conventional schemes are implemented using the simulation tool called network simulator 2.35. The front end language used to implement the protocols is Object oriented Tool Command Language (OTCL) respectively. The discrete events in the network scenarios are analysed and the constant bit rate traffic model is used for transmission. Packet rate delivery, energy consumption delay and false node detecting ratio are the parameters used for evaluation of proposed method and the conventional methods considered here are SCMM and SRCS. Remaining parameters used during simulation is given in the table 1.

4.1. Packet Rate Delivered. The delivery of packet rates is defined by taking the ratio of total number of sent packets and the total number of received packets. The successful delivery of sent packets with respect to their number of intermediate relay nodes is said to be packet rate delivered. Packet rate delivered (PRD) is evaluated by estimating the number of received packets at the

Parameter	Value
Number of nodes	100
Type of channel	Wireless channel
Simulation Area	1000X1000m2
Range of transmission	250 metres
Data-rate	11 Mbps
MAC type	IEEE 802.11
Network Interface Type	WirelessPhy

receiver end and it is given in equation 6,

$$P_R D = \sum_{n}^{m} = 0 TotalPacketSent/TotalPckRcvd \tag{6}$$

The packet delivery rates for the proposed method GE2SDT and the conventional schemes SCMM and SRCS are shown in figure 2. The proposed method GE2SDT has better delivery rates in terms of packets when compared with the SCMM and SRCS methods. This indirectly represents the proposed model has lower losses of packets. If the density of the nodes gets increased then simultaneously the rate of delivery of packets also gets increased.

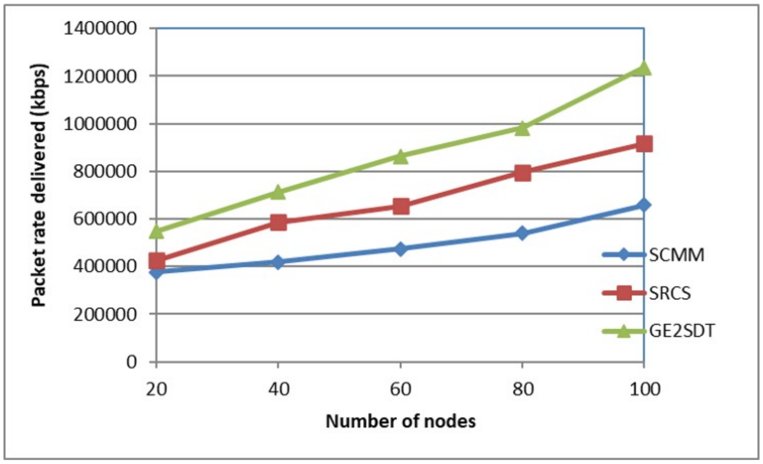

Figure 2. Packet Rate Deliveredl

4.2. AverageDelay. The average delay in terms of data transmission from the source point to the destination point is defined by evaluating the time difference between the sent time and received time of packets. This includes the evaluation of processing time includes queuing delay as well from one node to another. The average transmission delay of data transaction is calculated using equation 7 where n represents the number of nodes

$$Delay = \sum_{0}^{n} \frac{PckRcvdTime - PkdSndTime}{n} \tag{7}$$

Figure 3 shows the graphical representation of average transmission delay for the proposed scheme GE2SDT and the conventional methods SCMM and SRCS. Therefore the proposed scheme obtains lower data transmission delay when compared with the conventional protocols SCMM and SRCS.

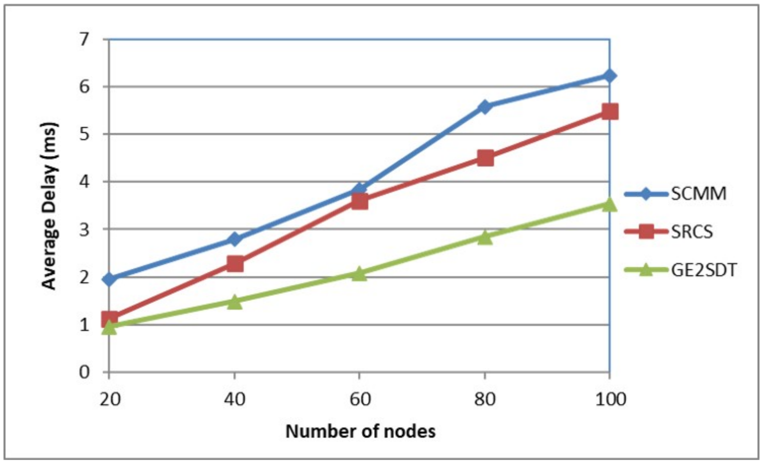

FIGURE 3. Average Delay

4.3. False Node Detection Ration. False Node Detection Ratio (FNDR) is defined as the evaluation of detection of malicious nodes from the deployed nodes in the network. By taking the computational ratio between the malicious nodes count and the normal nodes count the FNDR is computed. Normal nodes transmit the packets without any data loss or modifications but malignant nodes send false data to the destination with time delays. The graphical representation of both proposed scheme GE2SDT and the existing protocols SCMM and SRCS is shown in figure 5. The proposed method obtains better FNDR rate when compared with existing methods

4.4. Energy Consumption. The level of energy per node that is consumed during the data processing and transmission is said to be energy consumption of that particular node at some instant of time. Energy consumption calculation is computed for the detection of remaining energy level that is left in each node present in the network.

Figure 5 shows the graphical representations of energy consumption for both proposed GE2SDT and existing methods SCMM and SRCS. The proposed scheme

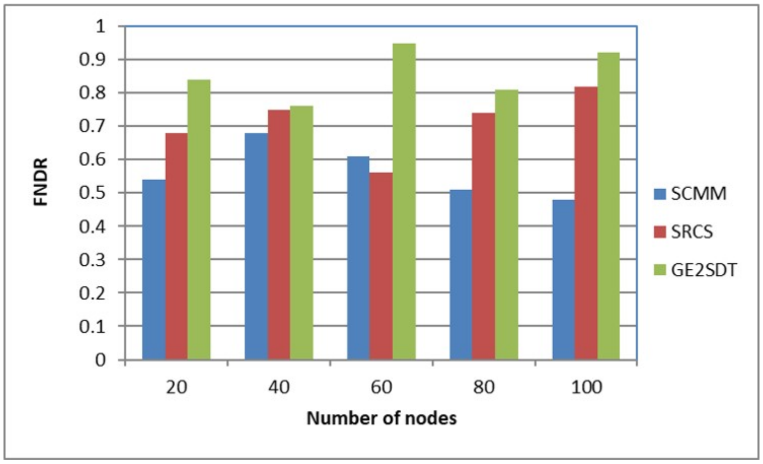

Figure 4. FNDR

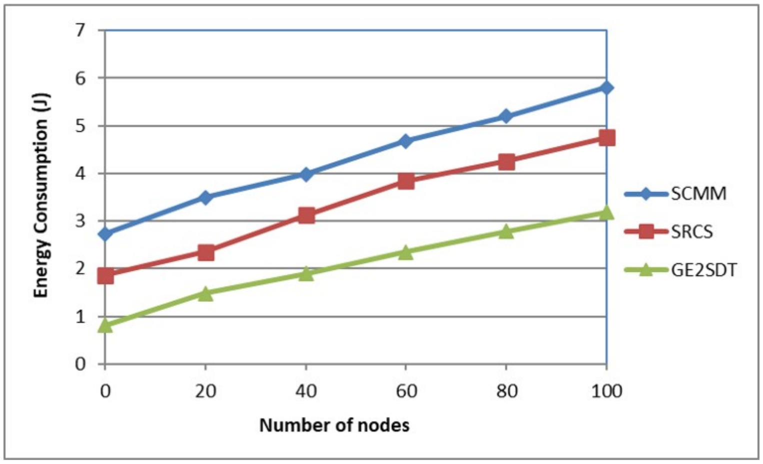

Figure 5. Energy Consumption

consumes lower energy when compared with the conventional methods. Thereby this proves that the selected routes are more reliable and resource constraint.

5. Conclusion

Grid based energy efficient and secured data transaction scheme is proposed here. Initially the cost function is evaluated to select the optimal nodes for carrying out the data transaction process. The network is split into equal number of grids and each grid is placed with certain number of nodes. The node cost function is estimated for all the nodes present in the network. Once the optimal energy proficient nodes are selected then the data transaction process is carried out in a secured way using malicious nodes filtration process. Secondly the cloud level data integrity is implemented by enabling partial private keys among cloud servers and users. Therefore, the message is transmitted in a secret sharing method to the end user and this process makes the network more efficient. Simulation analysis is carried out and the results are evaluated. The delivery rates and malignant node detection rate achieves better when compared to conventional methods. In future, the work is extended to implement in realistic scenario with combined effects of machine learning methods.

Conflicts of interest : The authors declare no conflict of interest.

Data availability : Not applicable

Acknowledgments : Authors are greatfully acknowledge the research supports received from Vels University, Chennai-600117, India.

References

1. A.A. Anasane, & R.A. Satao, *A survey on various multipath routing protocols in wireless sensor networks*, Procedia Computer Science **79** (2016), 610-615.
2. T. Qiu, X. Liu, L. Feng, Y. Zhou, & K. Zheng, *An efficient tree-based self-organizing protocol for internet of things*, Ieee Access **4** (2016), 3535-3546.
3. T. Qiu, Y. Lv, F. Xia, N. Chen, J. Wan, & A. Tolba, *ERGID: An efficient routing protocol for emergency response Internet of Things*, Journal of Network and Computer Applications **72** (2016), 104-112.
4. S. Pundir, M. Wazid, D.P. Singh, A.K. Das, J.J. Rodrigues, & Y. Park, *Intrusion detection protocols in wireless sensor networks integrated to Internet of Things deployment: Survey and future challenges*, IEEE Access **8** (2019), 3343-3363.
5. W.H. Hassan, *Current research on Internet of Things (IoT) security: A survey*, Computer networks **148** (2019), 283-294.
6. S.K. Lee, M. Bae, & H. Kim, *Future of IoT networks: A survey*, Applied Sciences, **7** (2017), 1072.
7. C. Stergiou, K.E. Psannis, B.G. Kim, & B. Gupta, *Secure integration of IoT and cloud computing*, Future Generation Computer Systems **78** (2018), 964-975.
8. V.B. Reddy, A. Negi, & S. Venkataraman, *Trust computation model using hysteresis curve for wireless sensor networks*, In 2018 IEEE SENSORS, 2018, 1-4.
9. A. Ahmed, K.A. Bakar, M.I. Channa, K. Haseeb, & A.W. Khan, *TERP: A trust and energy aware routing protocol for wireless sensor network*, IEEE Sensors Journal **15** (2015), 6962-6972.
10. X. Wu, J. Huang, J. Ling, & L. Shu, *BLTM: beta and LQI based trust model for wireless sensor networks*, IEEE Access **7** (2019), 43679-43690.
11. M. Shen, B. Ma, L. Zhu, R. Mijumbi, X. Du, & J. Hu, *Cloud-based approximate constrained shortest distance queries over encrypted graphs with privacy protection*, IEEE Transactions on Information Forensics and Security **13** (2017), 940-953.
12. S. Yao, Z. Li, J. Guan, & Y. Liu, *Stochastic cost minimization mechanism based on identifier network for IoT security*, IEEE Internet of Things Journal **7** (2019), 3923-3934.

13. S. Singh, & J. Sidhu, *Compliance-based multi-dimensional trust evaluation system for determining trustworthiness of cloud service providers*, Future Generation Computer Systems **67** (2017), 109-132.
14. N. Somu, G.R. MR, K. Kirthivasan, & S.S. VS, *A trust centric optimal service ranking approach for cloud service selection*, Future Generation Computer Systems **86** (2018), 234-252.
15. X. Li, Q. Wang, X. Lan, X. Chen, N. Zhang, & D. Chen, *Enhancing cloud-based IoT security through trustworthy cloud service: An integration of security and reputation approach*, IEEE Access **7** (2019), 9368-9383.
16. S. Siadat, A.M. Rahmani, & H. Navid, *Identifying fake feedback in cloud trust management systems using feedback evaluation component and Bayesian game model*, The Journal of Supercomputing **73** (2017), 2682-2704.
17. Huang, Longtao, Shuiguang Deng, Ying Li, Jian Wu, Jianwei Yin, and Gexin Li, *A trust evaluation mechanism for collaboration of data-intensive services in cloud*, Applied Mathematics & Information Sciences **7** (2013), 121-129.
18. Yasir Mehmoo, Ammar Oad, Muhammad Abrar et al., *Edge Computing for IoT-Enabled Smart Grid.Security and communication networks*, Hindawi 2021.
19. Khan, Lalith, Devi, Rajalakshmi, *A multi-attribute based trusted routing for embedded devices in MANET-IoT*, Microprocessor and Microsystems, 2022. https://doi.org/10.1016/j.micpro.2022.104446

L. Sasirega is a Ph.D. research scholar in the Department of Computer science, Vels Institute of Science, Technology, and Advanced Studies, Chennai, Tamil nadu, India. She is working as Assistant Professor in Kalaignar karunanithi arts and science college, Thiruvannamalai, Tamil nadu. She has published research papers in conferences and journals in national and international level. Here research interests include IoT, WSN and security.

Rsearch Scholar, Department of Computer Science, Vels Institute of Science, Technology and Advanced Studies, Tamil Nadu, India.
e-mail: lsasirega1975@gmail.com

C. Shanthi, Ph.D. is working as Associate Professor in the Department of Computer science, Vels Institute of Science, Technology, and Advanced Studies, Chennai, Tamil nadu, India. She has vast experiences in the teaching field. She has published her papers in various conferences and journals. Here research interests include computer networks, WSN, and information security.

Associate Professor, Department of Computer Science, Vels Institute of Science, Technology and Advanced Studies, Tamil Nadu, India.
e-mail: shanc08071978@gmail.com