Journal of ISMAC (2020)
Vol.02/ No. 02
Pages: 96- 105
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2020.2.003

Sensor Cloud Based Architecture with Efficient Data Computation and Security Implantation for Internet of Things Application

Dr. Abul Bashar
Department of Computer Engineering
Prince Mohammad Bin Fahd University
Kingdom of Saudi Arabia
Email: abashar@pmu.edu.sa

Abstract: The growth of the information and communication technology has led the world to experience more sophisticated service that were once thought to be a fantasy. The emergence of the internet of things has further taken the world one step ahead by enabling the tangible things around to communicate. The IOT affords to offer more advanced services by the incorporation of the wireless sensors. The collection of the information and its delivery in the platform of internet of things is taken care by the enormous number of smart devices present in it and the numerous of smart devices present cause a very high amount of data flow. The issue arises in such platforms of internet of things in handling, regulating, storing and computing the huge amount of data flow. Move over the security of the data are also uncertain. To manage all these the paper delivers a sensor cloud based architecture with highly efficient computation and the security implantation for the application of internet of things. The proposed model improves the computation capability and the security of the data by using cloud service, the machine learning and the encryption scheme. The network simulator -3 evaluates the performance of the delivered model that provides a satisfying and sustaining results than the existing methods. The experiments were carried out on the grounds of the longevity of the network, overhead in the transmission the amount of energy used and as well as the packet drop ratio. The results attained on each ground were found be 25%, 30%, 38.76% and 50.7% better compared to the state of art approaches.

Keywords: Sensor Networks, Sensor Cloud, Machine learning, Internet of Things, encryption scheme

1. Introduction

The sensor network that are capable of sending and receiving message without need of wired and infrastructure based communication technologies have become has attained a rapid prominence among a variety and a broad scope of applications. These tiny wireless sensors affords to sense an information with the help of the sensing element present in it, process it, using the microprocessor employed in it, store the information's using the limited amount of memory in and convey the messages sensed with the help of the transceiver fixed in it. The sensor performs all the above mentioned process with the battery that is source of power for the sensors.

ISSN: 2582-1369 (online)

Journal of ISMAC (2020)
Vol.02/ No. 02
Pages: 96- 105
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2020.2.003

These sensors that are capable of sensing the environmental changes, the operation of an industry, human activities, vehicle movement, availability of the stock in a department store, presence and absence of a student in the school, the health of the person, disaster areas , heath of machine etc., is incorporated with the Internet of things to deliver even more advanced services. Numerous of such sensors are linked with the applications of the internet of things and lay as the basic and primary source of information gathering in IoT, causing a very high amount of data flow. Handling these enormous amount of data flow are highly tedious and as well as challenging for the tiny sensors that are incapable of storing the huge amount and scaling the resources available in it.

The security provision of the data sensed also remains questioned as the internet of things engages numerous of heterogeneous devices and communicate in a distributed manner. This type communication extended through the IoT is untrustworthy and highly vulnerable malicious attacks. Apart from this however the IoT requires a strategy that minimize the energy usage, balances the load, improve the data delivery along with the network longevity and a reliable way of delivering data. Hence mounting an intellectual and in effect IOT communiqué scheme guaranteeing the security of the data and the retaining the consistency of the network is quiet challenging. The figure.1 depicts the overview of the proposed architecture.

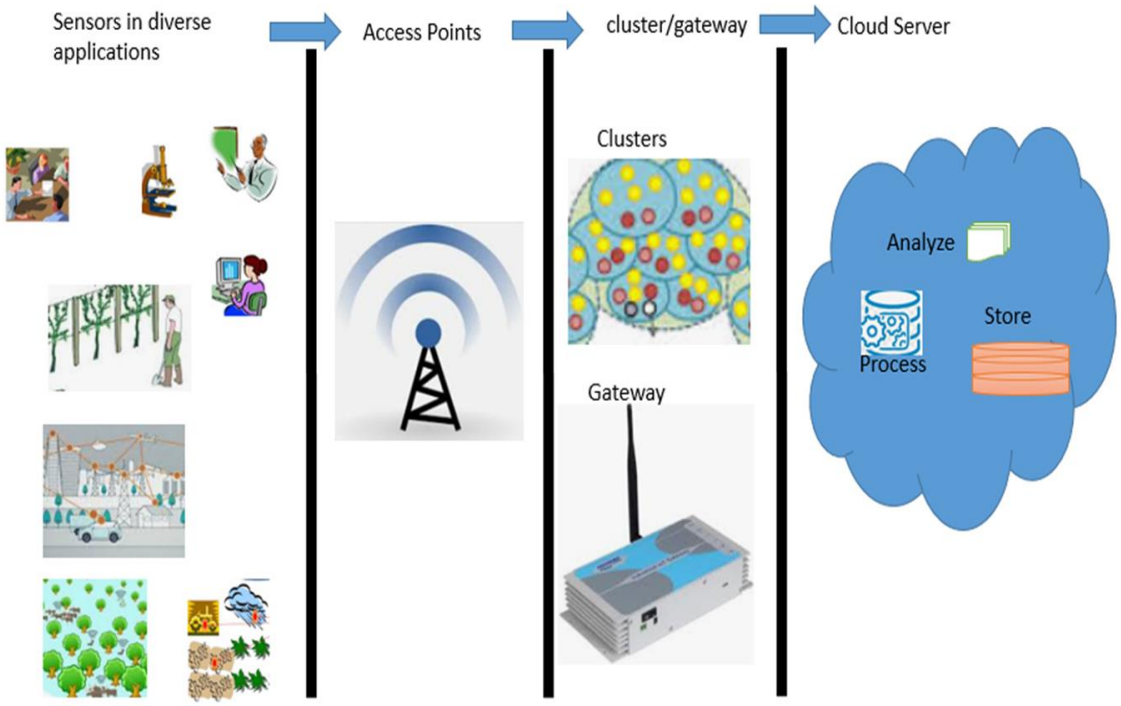

Figure.1 Proposed Architecture Overview

ISSN: 2582-1369 (online)

Journal of ISMAC (2020)
Vol.02/ No. 02
Pages: 96- 105
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2020.2.003

To handle all the above mentioned issues and as well provide an effective computation and improved security while communicating and preserving the data, the paper delivers a novel method, sensor based cloud frame work that guarantees the secureness of the data and the effective computation in the network. The strategy used in paper could be used in the smart environments, where multitudes of sensors with RFID are deployed in the dispersed manner. The information collected by these sensors are forwarded to the head of the cluster or the gate way node, that convey the data the base station. The base station linked to the cloud server using any one of the wireless communication technology such as Wi-Fi, 4G or 5G further forwards the data to the cloud over internet , the Sensor integrated with the IoT are combined with the cloud to make the storage, analysis , communication and maintenance easy. To minimize the loss of data and improve the computation and the security level the proposed method includes a reliable encryption scheme that provides better integrity protecting the privacy of the data.

The method laid out in the paper clusters the sensors according to its continuously varying pivotal positioning to balance the load and as well as enhance the longevity of the network. Utilizes the cloud architecture for storage and processing the data, and finally employs the node evaluation and the data protection scheme to sort out the endangered/malicious nodes to improve the constancy of the network and have an efficient data delivery respectively. This effective way of computation and security provision proceeds with the related works on the methodology previously devised and pit falls in it in 2. The proposed cloud based sensor, processing, storage and security in 3. The performance validation in 4. Conclusion in 5 followed by the reference.

2. Related works

As WSN has almost influenced an wide range of application with is sensing capabilities Ali et al [1] has presented a comprehended survey on the real word applications wireless sensor and its impacts on the fields such as surveillance, security, military, industry, education, agriculture, human activities etc., Nguyen, et al [2] managed the energy utilization of the internet of things applications using an efficient routing ware of energy harvesting. “WSN have capacity to trace out an unprecedented areas at a cost effective way, limited dimension and restricted energy consumption are prone to multitudes of attacks when routing the data gathered, the Shahzad, et al [3] devised a “energy aware routing and filtering node, selection to extend network lifetime in communicative cipher based en route filtering, in addition the distance to the destination, the residual energy are considered to minimize the energy utilization”

Abdelwahab et al [4] proposed the cloud of thing to provides service on sensing the utilizing the entire resources of the internet of things to deliver the telemetry sensing, the method laid out in [4] allowed a distributed computation, insightful data examination and decision making by developing a “sensing

ISSN: 2582-1369 (online)

Journal of ISMAC (2020)
Vol.02/ No. 02
Pages: 96- 105
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2020.2.003

resource discovery and virtualization algorithm – SRDVD." Zhu, et al [5] introduced the cloud with the social sensing capability to address the sustainability issues with the initiatives put out to minimize the carbon foot print.

Mehmood et al [6] presents the "knowledge centered context aware strategy to handle the intrusions generated by the malicious nodes" this address the security issues of the WSN that are liable of security breaches. "The vision of the future internet is laid out with heterogeneous computing devices and are linked together to form a network called internet of things, the trust in the IoT conveyance are questionable and unaddressed "Din, et al [7] presented the survey examining the extensive progress of the IoT along with the techniques that enable trust in the internet of things the pros and cons. He in his next paper [8] presented the design methodologies for the smart cities using the machine learning.

Raj, Jennifer S et al [9] in her paper presented the service quality optimized effective routing for the data sensed using the wireless sensor that were laid as the basic elements in the internet of things applications. Kumar, R. et al [10] provided the synopsis of the internet of things with the scope of delivering the architecture, the algorithms and the issues associated with the application of the IoT.

Bashar et al [11] conducted the "Intelligent Development of Big Data Analytics for Manufacturing Industry in Cloud Computing." Sathesh, A. et al [12] put forth the. "Optimized Multi-Objective Routing For Wireless Communication with Load Balancing." Duraipandian, M., and R. Vinothkanna et al [13] focused much in developing an internet of things based on the cloud to have an smart home environment by embedding an identification tag for every physical things laying around and allowing them to communicate to cloud over internet.

3. Proposed Effective Computation and Security Implantation

The laid out process involves various stages as shown in the flowchart presented in the figure.2 the sensors deployed in tracing out the changes in the smart environment is grouped according constant variations in the pivotal positions. The unsupervised ML the k-means is employed in the laid out process to group the sensors and form clusters. The sensors engaged are segregated into "centroid based regions" and are formed as cluster according to the location of the sensors, every sensor is identified with the radio frequency identification Tag,

ISSN: 2582-1369 (online)

Journal of ISMAC (2020)
Vol.02/ No. 02
Pages: 96- 105
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2020.2.003

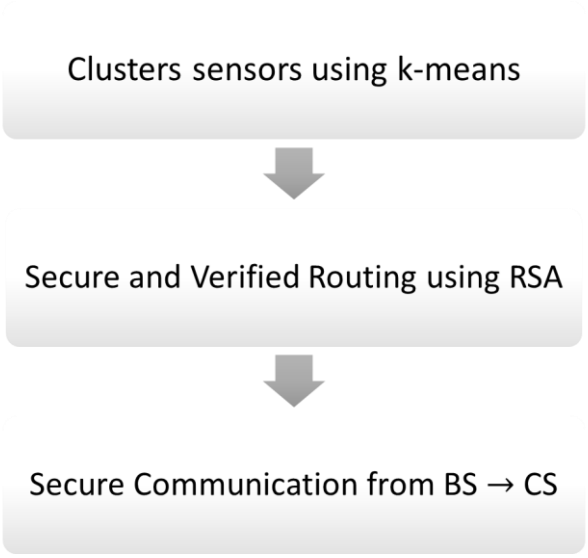

Figure .2 Flow Chart for Proposed

3.1. Clustering of Sensor

The K-means [14] strategy works on the principle of expectation and maximization to solve a problem, the clustering is followed in the proposed process to balance load in the network, avoid network congestion and enhance the network longevity. It starts by specifying the cluster 'K' and then initializes the centroids, following a shuffling and randomly choosing the 'K' data points for the center points or the centroids. This is done without interchanging. This process is iterated until no changes are observed in the center points. Determine the distance across the data points and the centroids according to the equation 1 shown below

$$distance = (distance\ across\ datapoits\ and\ centroids)^2 \quad (1)$$

Allocate every data point to the nearest cluster (centroid), process the centroids for the cluster by taking the average of every data points belonging to the cluster. The expectation allocates the data points to the nearest cluster and the maximization enables to determine the centroids of the every cluster. The equation 2 and 3 are the Expectation and Maximization step.

$$Expectation = \sum_{i=1}^{m} \sum_{k=1}^{k} \| Cluster^{\,i} - center_{\,point} \| \text{^}2 \quad (2)$$

ISSN: 2582-1369 (online)

Journal of ISMAC (2020)
Vol.02/ No. 02
Pages: 96- 105
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2020.2.003

$$Maximization\ = 2\sum_{i=1}^{m} data\ points(Cluster^{\,i} - center_{\,point}\ )\text{^}2 \quad (3)$$

The new assignments are reflected by reprocessing the centroids, of each cluster.

Head for the each cluster is assigned to convey the information from the sensors to the cloud, the further the information conveyed to the cloud is stored in the cloud and the for the purpose of processing and re-claiming.

3.2. Secure Communication between Base Station and Cloud

An asymmetric centered encryption is followed technique is followed in the proposed method. To secure the data conveyed. The encryption process is as follows.

i. The cloud server and the base station generates the pair of keys, ($key_{\,cs}$ and $Key_{\,bs}$)
ii. Where the $p\ key_{\,cs}$ represents the $ukey_{\,cs}$ represents the public and the private key of the cloud server respectively. Similarly the keys are assigned for the base station.
iii. The $p\ key$ are used for encrypting and are shared through the directory allotted for the public usage, in the cloud, more over the ID and the stored $p\ key$ are clubbed. During this process the $u\ keys$ are left undisturbed.
iv. The RSA based cryptography is followed in the method to encrypt and decrypt the information's, the steps involved are
    a. Produce 2 distinct keys.
    b. Choose two primes number (A and B).
    c. Take the product of primes Prod (AxB).
    d. Compute$\lambda\ (prod)$.
    e. Choose co-prime 'C' to $\lambda\ (prod)$ for (1< C< $\lambda\ (prod)$ and GCD (C, $\lambda\ (prod)$).
    f. Determine modular multiplicative inverse for co-prime 'C' (C^{-1} | $\lambda\ (prod)$ |).
    g. Produce the $p\ key$ (C^{-1} | $\lambda\ (prod)$ |), $prod$) and $u\ keys$ ($C, prod$).
    h. Perform encryption from BS→CS using encryption = $data^{\,c}$ |$prod$ |.
    i. Decryption is done using the decryption = encryption$^{C^{-1}\,|\,\lambda\,(prod)\,|}$ |$prod$ |.
    j. Cluster head authentication is performed by applying the XOR operation across the key and the Data that is sent to produce the signature to authenticate or to obtain the MAC.
    k. The XOR results are summed up with the actual data to be transmitted from BS→CS.
    l. If true the verification and the authentication takes place for the cluster else ignores the head of the cluster.

ISSN: 2582-1369 (online)

Journal of ISMAC (2020)
Vol.02/ No. 02
Pages: 96- 105
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2020.2.003

4. Performance Assessment

The laid out model was simulated using the network simulator-3 with random number of sensors ranging from 100 to 500 deployed over the square spotting area. With number of malicious node in the network assumed to be 10 and was distributed randomly. “The malevolent node send the incorrect route reactions and direct the data packets to unlicensed nodes or the data packets can be lost. Public keys are usually identified by all sensors through a PAD-publicly accessible directory built on the cloud server, but private keys need not be dispersed and thus cannot be cooperated. Every nodes excluding the BS have limited memory, storing, computing and battery power limitations. Transmission capacity for every node is set as twenty meters. Initially all nodes have a common 5 J energy resource”. Each packet size is fixed as 20 bits and the pay load size is fixed as 512 bytes. The UDP protocol is used in the transport layer, the evaluation results are compared with the prevailing methods such as the SEID [6], SEER [15] and the SLEACH [16]

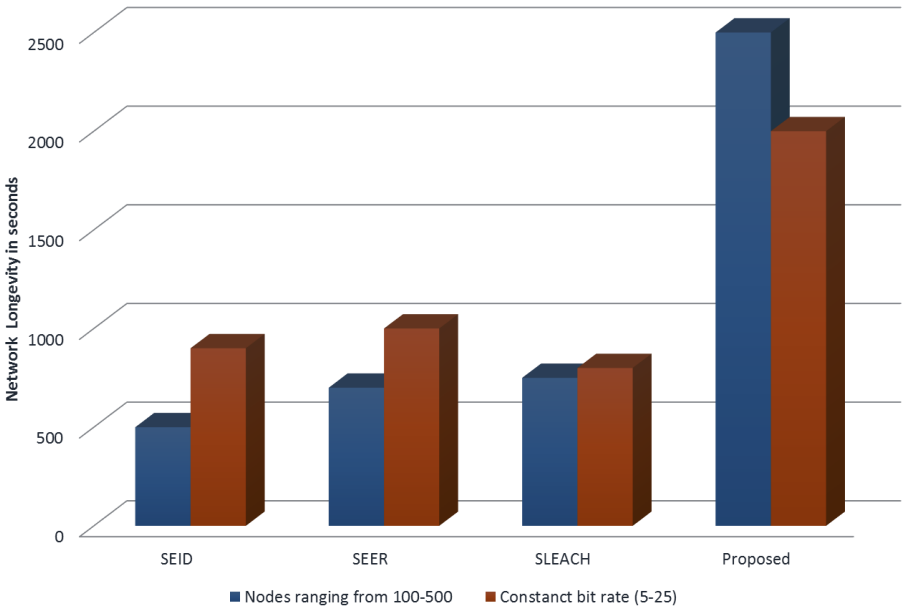

Figure.3 Network Longevity for a Varying Nodes and Constant Bit Rate

The results depicted in figure.3 for the network longevity proves that the proposed method has a 25% better longevity compared to the existing methods SEID, SEER and SLEACH. The proposed method is more streamlined compared to the existing, in terms of transmission over head, and an enhanced network longevity.

ISSN: 2582-1369 (online)

Journal of ISMAC (2020)
Vol.02/ No. 02
Pages: 96- 105
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2020.2.003

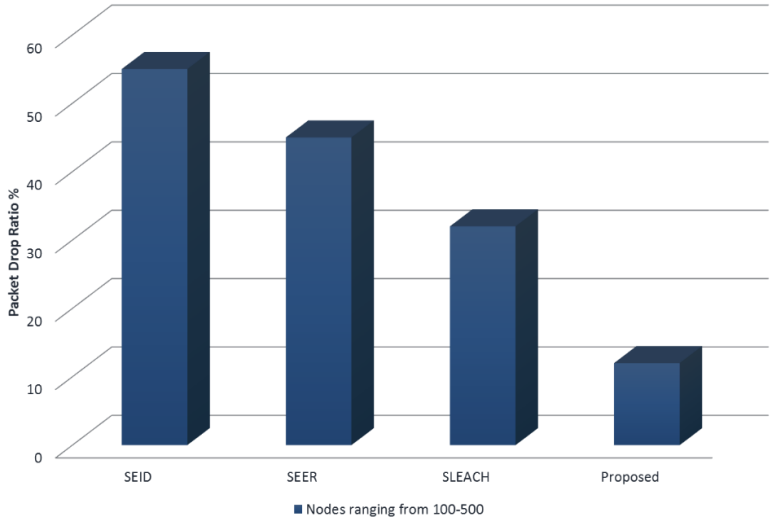

Figure.4 Drop Ratio of Packets

The figure .4 depicts the drop ratio of packets for the proposed method. The results observed proves to provide a 50 % higher PDR compared to the existing and also experience the decrease of PDR in the presence of the malicious nodes.

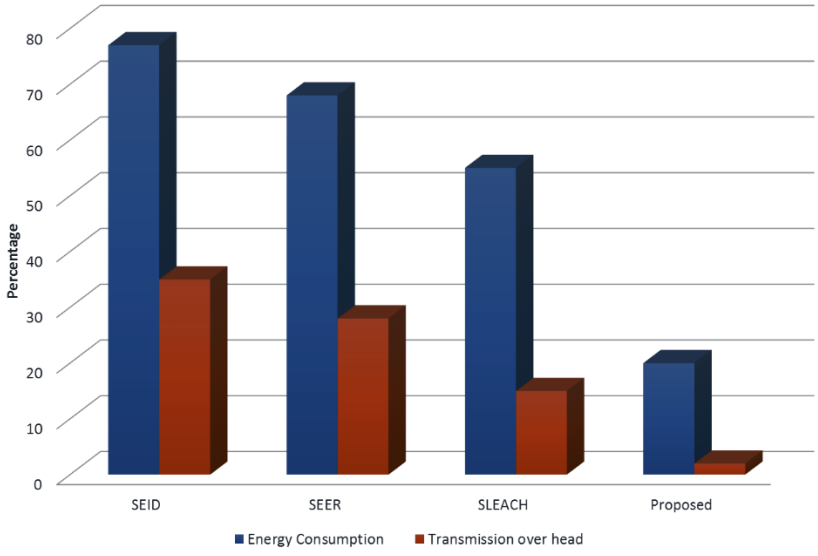

Figure.5 Energy Consumption and Transmission over head

ISSN: 2582-1369 (online)

Journal of ISMAC (2020)
Vol.02/ No. 02
Pages: 96- 105
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2020.2.003

The results in figure.5 presents the energy consumption and the transmission overhead observed for the proposed method and the existing methods, the proposed methods affords to offer an 38.6%and 30 % improvement compared to the existing.

5. Conclusion

The cloud based sensor architecture, provides an effective computing and security enhancements in conveying the data from sensor to cloud using the clustering based on unsupervised learning and security provision using RSA. The simulation results obtained evinces the improved performance of the proposed scheme over the existing on the grounds of the power consumption, PDR, transmission overhead and network longevity.

Reference

[1] Ali, Ahmad, Yu Ming, Sagnik Chakraborty, and Saima Iram. "A comprehensive survey on real-time applications of WSN." Future internet 9, no. 4 (2017): 77.

[2] Nguyen, Thien D., Jamil Y. Khan, and Duy T. Ngo. "An effective energy-harvesting-aware routing algorithm for WSN-based IoT applications." In 2017 IEEE International Conference on Communications (ICC), pp. 1-6. IEEE, 2017.

[3] Shahzad, Muhammad K., and Tae Ho Cho. "An energy-aware routing and filtering node (ERF) selection in CCEF to extend network lifetime in WSN." *IETE Journal of Research* 63, no. 3 (2017): 368-380.

[4] Abdelwahab, Sherif, Bechir Hamdaoui, Mohsen Guizani, and Taieb Znati. "Cloud of things for sensing-as-a-service: Architecture, algorithms, and use case." IEEE Internet of Things Journal 3, no. 6 (2016): 1099-1112.

[5] Zhu, Chunsheng, Victor CM Leung, Joel JPC Rodrigues, Lei Shu, Lei Wang, and Huan Zhou. "Social sensor cloud: framework, greenness, issues, and outlook." IEEE Network 32, no. 5 (2018): 100-105.

[6] Mehmood, Amjad, Akbar Khanan, Muhammad Muneer Umar, Salwani Abdullah, Khairul Akram Zainol Ariffin, and Houbing Song. "Secure knowledge and cluster-based intrusion detection mechanism for smart wireless sensor networks." IEEE Access 6 (2017): 5688-5694.

[7] Din, Ikram Ud, Mohsen Guizani, Byung-Seo Kim, Suhaidi Hassan, and Muhammad Khurram Khan. "Trust management techniques for the Internet of Things: A survey." IEEE Access 7 (2018): 29763-29787.

ISSN: 2582-1369 (online)

Journal of ISMAC (2020)
Vol.02/ No. 02
Pages: 96- 105
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2020.2.003

[8] Din, Ikram Ud, Mohsen Guizani, Joel JPC Rodrigues, Suhaidi Hassan, and Valery V. Korotaev. "Machine learning in the Internet of Things: Designed techniques for smart cities." Future Generation Computer Systems 100 (2019): 826-843.

[9] Raj, Jennifer S. "QoS optimization of energy efficient routing in IoT wireless sensor networks." Journal of ISMAC 1, no. 01 (2019): 12-23.

[10] Kumar, R. Praveen, and S. Smys. "A novel report on architecture, protocols and applications in Internet of Things (IoT)." In 2018 2nd International Conference on Inventive Systems and control (ICISC), pp. 1156-1161. IEEE, 2018.

[11] Bashar, Abul. "Intelligent Development of Big Data Analytics for Manufacturing Industry in Cloud Computing." Journal: Journal of Ubiquitous Computing and Communication Technologies September 2019, no. 01 (2019): 13-22.

[12] Sathesh, A. "Optimized Multi-Objective Routing For Wireless Communication with Load Balancing." Journal of trends in Computer Science and Smart technology (TCSST) 1, no. 02 (2019): 106-120.

[13] Duraipandian, M., and R. Vinothkanna Mr. "Cloud Based Internet of Things for Smart Connected Objects." Journal of ISMAC 1, no. 02 (2019): 111-119.

[14] https://towardsdatascience.com/k-means-clustering-algorithm-applications-evaluation-methods-and-drawbacks-aa03e644b48a

[15] Das, Ayan Kumar, Rituparna Chaki, and Kashi Nath Dey. "Secure energy efficient routing protocol for wireless sensor network." Foundations of Computing and Decision Sciences 41, no. 1 (2016): 3-27.

[16] El_Saadawy, Mona, and Eman Shaaban. "Enhancing S-LEACH security for wireless sensor networks." In 2012 IEEE International Conference on Electro/Information Technology, pp. 1-6. IEEE, 2012.

Biography: Dr. Abul Bashar is currently working as Assistant Professor at Prince Mohammad Bin Fahd University, Kingdom of Saudi Arabia in the College of Computer Engineering and Sciences. Earlier, he completed his PhD from the School of Computing and Information Engineering at the University of Ulster, Coleraine, UK in 2011. He received his B.E. degree in Electronics & Communication Engineering from Osmania University, Hyderabad, India in 1995. He has an M.S. degree in Electrical Engineering from King Fahd University of Petroleum & Minerals (K.F.U.P.M.), Dhahran, Kingdom of Saudi Arabia in 1999. Before joining his PhD research he was a Lecturer for 8 years in the Electrical Engineering department at K.F.U.P.M. He is a recipient of Osmania University Engineering Gold Medal in 1995, M.S. Research Scholarship from KFUPM (1996) and Vice Chancellors Research Scholarship from University of Ulster (2008). He is actively involved in the TPC/Review committees of renowned journals and conferences namely CSC IJCN, IEEE WCNC 2011, ISCI 2011, ICDIPC 2011, ICSECS 2011, DICTAP 2011 and NDT 2009/2010/2012.

ISSN: 2582-1369 (online)