iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** X **Month of publication:** October 2018

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue X, Oct 2018- Available at www.ijraset.com

Evaluate and Propose Energy Efficient Approach for Data Aggregation in IoT

Shikha Thakur
Himachal Pradesh University

Abstract: ***The IOT network is the decentralized type of network which can sense the information and pass it to base station. Due to small size of the sensor nodes, the energy consumption is the major issue of the network. The LEACH is the energy efficient protocol which can divide whole network into fixed size clusters. In each cluster, cluster heads are selected which can transmit data to base station. The LEACH protocol is the dynamic clustering protocol in which cluster heads are changes after each round in the network. In this research work, the LEACH protocol is improved to reduce energy consumption of the wireless sensor networks. In the proposed improvement, the cache nodes are deployed which can aggregate data from the cluster heads and then pass data to base station. The simulation of the proposed technique is done in MATLAB and results are compared with the existing approach in terms of certain parameters. It is analyzed that proposed technique performs well as compared to existing technique.***

Keywords: IoT, LEACH, Clustering, Gateway

I. INTRODUCTION

IoT stands for internet of things which is termed by the of the Radio Frequency Identification (RFID) development community. It is defined as the network in which physical objects are connected to each other. Internet is not only the network for the connectivity but also evolve the network of device of all type and sizes, vehicles, smart phones, home appliances, toys, cameras, and many more. The IoT applications provide Internet and various advance software and communication services. Here, the objects can be connected to each other or to the things and can access the media present [1]. The objects and things present worldwide can be interlinked with each other and provide access to communication in order to provide IoT environment. Being the part of small computer is the main criteria for each object or thing. Any kind of forecast present has been outperformed by the microchip to which the connection is made. It involves various technologies such as RFID, sensor and actuator, miniaturization, nanotechnology and smart entities. IoT can be defined into three categories such as (1) People to people, (2) People to machine /things, (3) machine to machine, which are interacting through internet [2]. The main objective here is to interconnect all the things present within this self-configuring wireless network which includes numerous sensors. An object that gets involved within a communication chain is also present. The combination of communication capabilities which are given by the data transmission is given by these lines present. RFID is known to be the main object within the IoT. The building of global infrastructure for RFID tags which is known to be a wireless layer present on the top of Internet. The communication is made amongst network of interconnected objects and the interconnected computers. There is a different Internet Protocol (IP) location for the objects at some instants [3]. These objects are embedded within the complex systems. In order to gather the information here, the various sensors are used which gather information related to temperature, and other aspects present in the surroundings. The sensors present near to each other transfer the gathered information in order to provide further processing as per the requirements of the current applications. In the recent year very much importance is given to the Security and privacy as it protects the data from any theft. Protection of data is very much necessary with the increase in the growth of the data nowadays, hence various mechanism are invented to minimize the major limitation of IoT. Security within these systems is always major concerns as there are numerous systems involved during the communication being held [4]. Thus, the data involved within these systems is to be made secure. Various data isolation techniques are provided here which can help in providing encryption measures within the systems. With the application of these systems it can be made sure that the data being transmitted to the destination reaches there without any modifications or stealing of important information by the unauthorized access. One of other major concerns within these systems is the violation of privacy of data present in them. In order to ensure that only the authorized users are given access to the private information, various algorithms are proposed here which can ensure that no unauthorized users have access to this information. Misdirection attack [5]: It is the attack in which packets are routed by the attacker to its children to other distant nodes but do not transfer to its legitimate parent. The main purpose of the intruder is to increase the latency by misdirecting the incoming messages due to which few packets are prevented from reaching the base station. The most popular Denial of Service Attack is the Misdirection attack. It changes the path of the packets in order create confusion

among nodes. Misdirection attacks are of different types and can be performed in two ways. “Packets forwarded to a node large away from the destination” is the type of misdirection attack which is very dangerous as forwarded packets are transferred to a sensor node which is far away and prevents packets to reach the destination timely [6]. It decreases the throughput and increases the delay infinitely. “Packets forwarded to a node close to actual destination” is the attack that is less intense as compared to previous one because it took long route to transfer packets to its destination node. Due to which there is increase in delay and decrease in throughput.

II. LITERATURE REVIEW

1) *Yogeesh Seralathan, et.al (2018)* presented all the devices in the internet of things are controlled and connected with the help of internet. Large number of sensitive data is being processed by the devices due to which the use of IoT devices increases widely. In order to large number of botnets, Malware like Mirai is widely used nowadays [7]. This malware has been utilized in DDoS attacks as well in which every second up to 1.2 Terabytes of networks traffic is generated. They performed various experiments, in order to determine compromise done by an IoT device’s in case of threat for the security and privacy of the data and they provide a case study of an IP camera. They also presented the importance of securing IoT and provide essential security practices for mitigating device exploitation.
2) *Chalee Vorakulpipat, et.al (2018)* presented the critical issue currently faced by the devices due large utilization of these devices. The major issue faced currently is the issue of the network security in the devices [8]. The use of devices nowadays increased drastically in order to access the corporate networks due to which they are prone to the major security risks. It is very necessary to use more services as most of the people are shifted from personal computers to mobile devices that lead to widely utilization of the IoT devices. They presented a concerns related to IoT security, reviews, and challenges faced by the devices as well as discussed the three generations of the IoT security.
3) *Jesus Pacheco, et.al (2017)* presented a framework for the security of IoT for the integration of a Smart Water Systems in the IoT, in a secure way. There are four layers in this used framework such as devices, communication, service, and application layers [9]. They also presented a methodology for the development of a threat model and this model has been utilized for the identification of the potential attacks against each layer, their effects of the devices and methods to mitigate and recover from these attacks. As per analysis, it is demonstrated that proposed approach of ABAIDS can detect both known and unknown attacks with high detection rates and low false positive alarms. They also have insignificant overhead in terms of memory and CPU usage. Proposed method protects the normal operation of the gateway in order to provide the availability.
4) *Se-Ra Oh, et.al (2017)* presented a connected, intelligent and context-aware device that works collectively known as internet of things (IoT). The IoT devices are growing quickly in the recent years as it provides the common functions of IoT devices that are helpful to all. Security is the main consideration in the IoT devices as they are more vulnerable to attacks and directly affect the IoT device in the IoT platform [10]. In the interworking process, they are more prone to critical influence in all connected IoT platforms. The security architecture of the oneM2M was discussed in this paper. Therefore, they developed an OAuth 2.0-basedoneM2M security component in order to provide authentication and authorization which is necessary for the security of IoT and for the protection of interworking between IoT platforms.
5) *U. M. Mbanaso, et.al (2017)* presented a novel configurable policy-based specification and the threats and vulnerabilities faced by an IoT system were analyzed. This specification has been utilized to scale proportionately in solving trust confidentiality and privacy issues in distributed environments [11]. A mechanism was proposed by author in this paper by which all the IoT entities can express their capabilities and requirements. For the negotiation of provable attributes and resources they constructed a fine-grained policy mutually. In order to solve the dispute resolution and auditable, they provide a mechanisms which solve the issues such as trust, privacy and confidentiality in a unified manner. This method provides a greats success in the IoT environments.
6) *Yiqun Zhang, et.al (2018)* presented it a major challenge for the IoT devices to support different cryptographic algorithms and standards within the physical constraints. In the Internet of Things security is the most important factor that need for the consideration. Author proposed a Recryptor in this paper which is are configurable cryptographic processor which utilizes its computational capabilities in order to enhance the existing memory of a commercial general-purpose processor [12]. A 10-transistorbitcell supports, in-memory bitline computing for the support of different bitwise operations up to 512-bits wide. The programmability of the Recryptor’s was demonstrated by implementing the cryptographic primitives of various public/secret key cryptographies and hash functions. 6.8% average speedup and 12.8% average energy was achieved by Recryptor running at 28.8 MHz in 0.7 V as compared to software- and hardware.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue X, Oct 2018- Available at www.ijraset.com

A. Experimental Results

The IoT network is the self-configuring network in which sensor nodes sense information and pass it to base station. Due to decentralized nature of the network, energy consumption, data aggregation and security are three major issues of the networks. This research work is focused on the energy consumption of the wireless sensor networks. The energy consumption issues is raised due to small size of the sensor nodes. The clustering is the efficient approach which increase lifetime of the sensor networks. In the clustering approach, the whole network is divided into fixed size clusters. The cluster heads are selected in each cluster and sensor nodes in each cluster will aggregate data to cluster head. The cluster head will transmit data to the base station. To increase lifetime of the sensor network, the optimization is proposed in the LEACH protocol. In the proposed approach, the cache nodes are deployed between the cluster head and base station. The cluster heads will transmit the data to nearest cache node and then cache send data to the base station. The cache aggregate data from the nearest cluster head. The distance between the gateway node and cluster head is calculated using Euclidian distance formula.

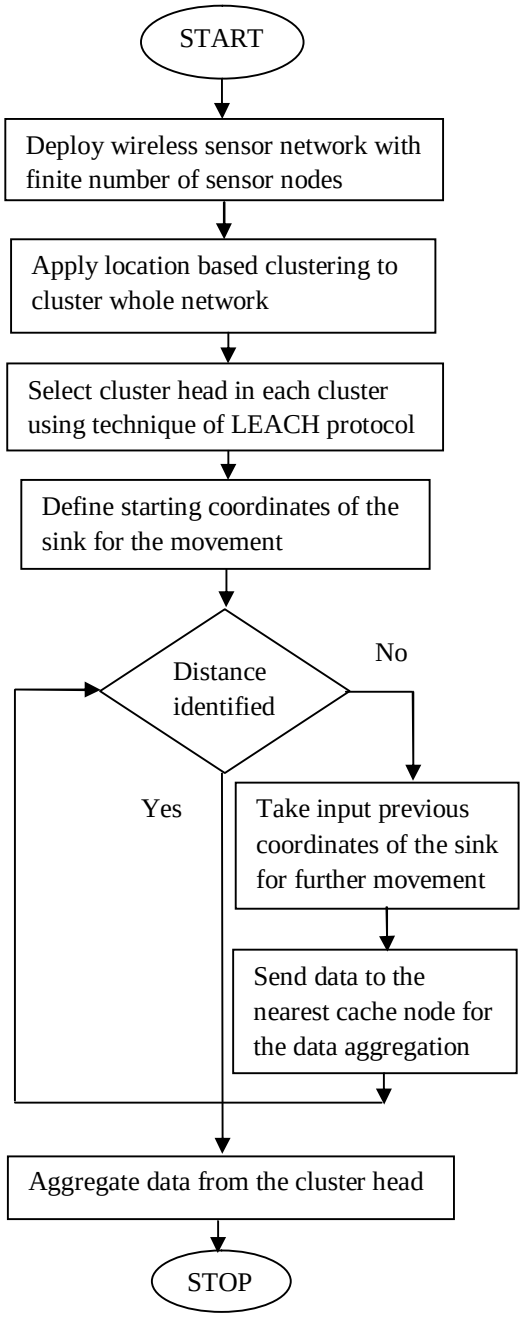


Figure 1: Proposed Flowchart

B. Experimental Results

The proposed work is implemented in MATLAB and the results are evaluated by making comparisons against proposed and existing work in terms of several parameters.

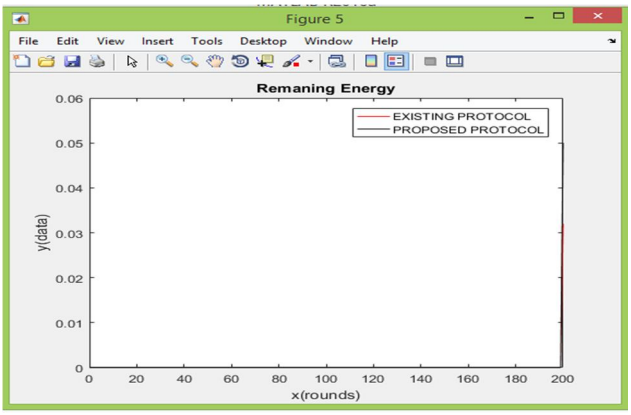


Fig 2: Energy Consumption

Figure 2 represents the comparison of basepaper and proposed technique. It results that the proposed protocol has minimum amount of energy consumption in comparison to the other techniques.

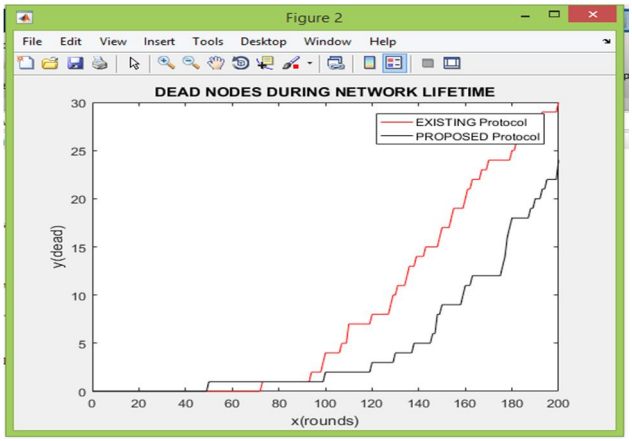


Fig 3: Number of dead Node Comparison

Figure 3 demonstrates the comparison between LEACH protocol and cache technique in terms of the dead nodes. The proposed technique has fewer amounts of dead nodes in the give amount of rounds.

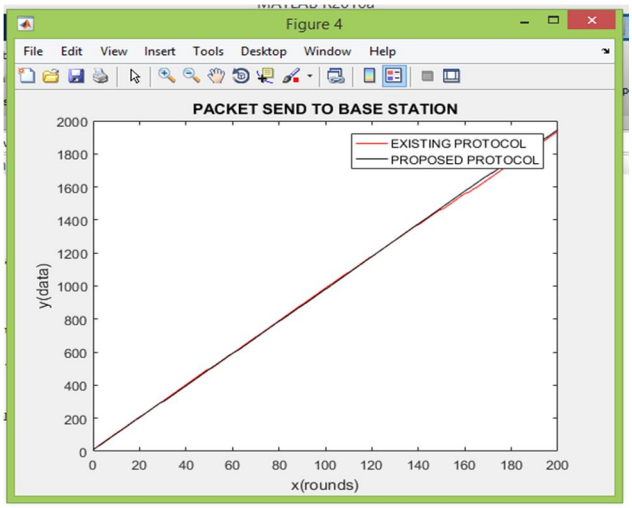


Fig 4: No of Packets Transmitted

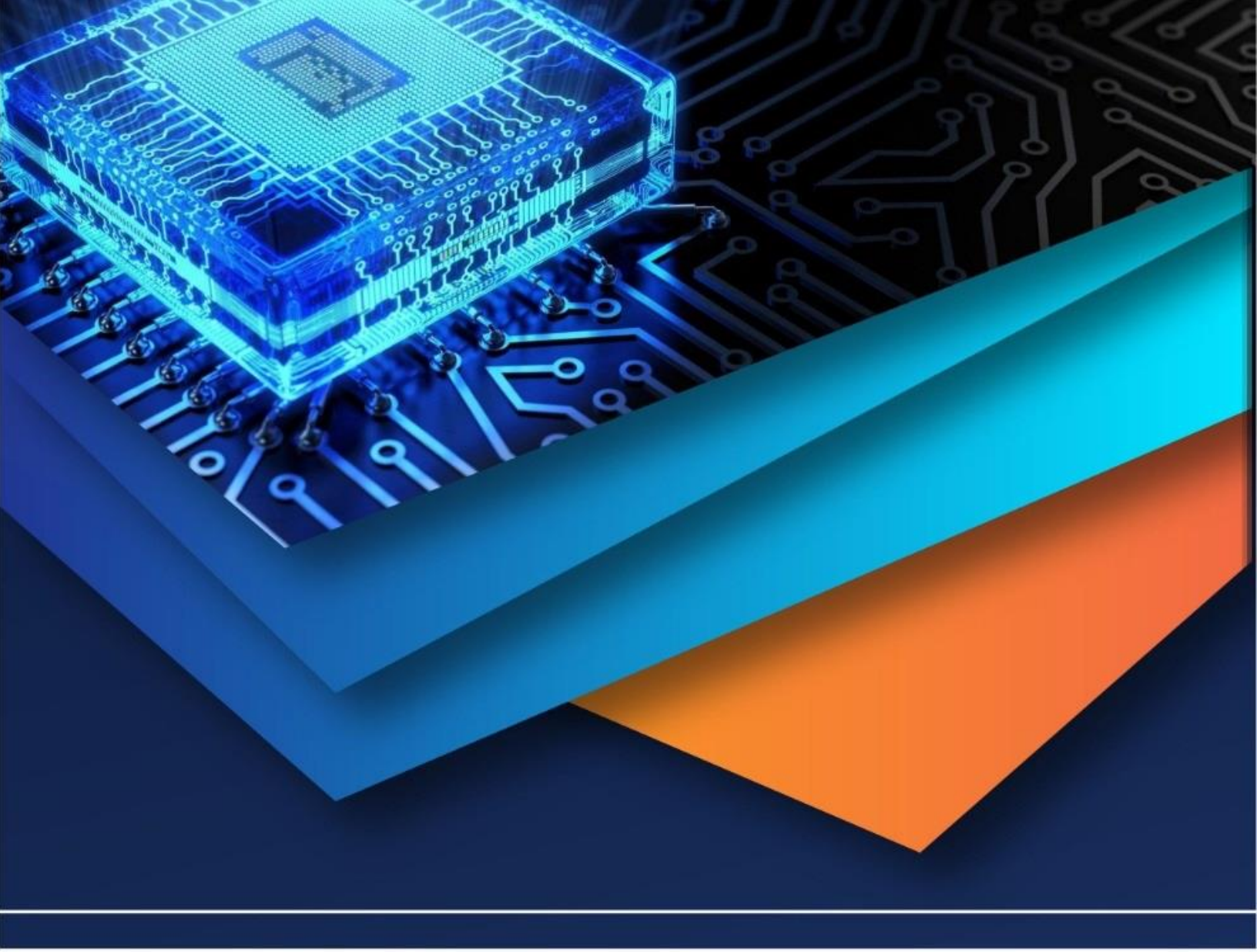
Figure 4 shows the comparison between the number of packet transmitted to the base station, proposed technique, base paper, LEACH and cache technique. The proposed technique transmits the large number of packet in comparison to the other techniques.

III. CONCLUSION

In this research work, it is concluded that due to dynamic nature of the IOT network energy consumption is the major issue which need to resolve. The clustering is the efficient approach which divide whole network into fixed size clusters and cluster heads are selected in each cluster. The cluster heads are selected on the basis of distance and energy. The sensor node which has minimum distance and maximum energy is selected as the cluster head. In this research work, the LEACH protocol is improved with the gateway node. The cache node will aggregate data from the cluster head. The cluster head transmit data to base station which is static in nature. The simulation of the proposed and existing technique is done in MATLAB and it is analyzed that proposed technique perform well in terms of remaining energy and number of dead nodes.

REFERENCES

[1] S. Sicari, A. Rizzardi , L.A. Grieco , A. Coen-Porisini, “Security, privacy and trust in Internet of Things: The road ahead”, Computer Networks, vol. 56, pp. 133-151, 2015.
[2] Arbia Riahi Sfar, Enrico Natalizio, Yacine Challal, Zied Chtourou, “A Roadmap for Security Challenges in Internet of Things”, vol. 12, pp. 15-21, 2017.
[3] Kim Thuat Nguyen, Maryline Laurent, Nouha Oualha, “Survey on secure communication protocols for the Internet of Things”, Ad Hoc Network, vol. 7, pp. 5-15, 2015.
[4] David Linthicum, “Responsive Data Architecture for the Internet of Things”, IEEE Computer, Vol 49, Issue 10, pp. 72-75, October 2016.
[5] Dongsik Jo and Gerard Jounghyun Kim, “ARIoT: Scalable Augmented Reality Framework for Interacting with Internet of Things Appliances Everywhere”, IEEE Transactions on Consumer Electronics, Vol. 62, Issue. 3, pp. 334-340, August 2016.
[6] Xinlie Wang, Jianqing Zhang, Eve. M. Schooler, “Performance evaluation of Attribute-Based Encryption: Toward data privacy in the IoT”, Communications (ICC), 2014 IEEE International Conference, vol. 19, issue 3, pp. 56-88, 2014.
[7] Yogeesh Seralathan, Tae (Tom) Oh , Suyash Jadhav, Jonathan Myers, Jaehoon (Paul) Jeong+, Young Ho Kim, and Jeong Neyo Kim, “IoT Security Vulnerability: A Case Study of a Web Camera”, International Conference on Advanced Communications Technology(ICACT), IEEE, vol. 13, issue 9, pp. 16-30, 2018.
[8] Chalee Vorakulpipat, Ekkachan Rattanalerdnusorn, Phithak Thaenkaew, Hoang Dang Hai, “Recent Challenges, Trends, and Concerns Related to IoT Security: An Evolutionary Study”, International Conference on Advanced Communications Technology(ICACT), vol. 7, issue 4, pp. 14-33, 2018.
[9] Jesus Pacheco, Daniela Ibarra, Ashamsa Vijay, Salim Hariri, “IoT Security Framework for Smart Water System”, 2017 IEEE/ACS 14th International Conference on Computer Systems and Applications, IEEE,vol. 9, issue 3, pp. 11-30, 2017.
[10] Se-Ra Oh, Young-Gab Kim, “Development of IoT Security Component for Interoperability”, IEEE, vol. 12, issue 4, pp. 67-89, 2017.
[11] U. M. Mbanaso, G. A. Chukwudebe, “Requirement Analysis of IoT Security in Distributed Systems”, 2017 IEEE 3rd International Conference on Electro-Technology for National Development (NIGERCON), IEEE, vol. 5, issue 7, pp. 20-30, 2017.
[12] Yiqun Zhang, Li Xu, Qing Dong, Jingcheng Wang, David Blaauw, and Dennis Sylvester, “Recryptor: A Reconfigurable Cryptographic Cortex-M0 Processor With In-Memory and Near-Memory Computing for IoT Security”, IEEE JOURNAL OF SOLID-STATE CIRCUITS, vol. 9, issue 3, pp. 25-56, 2018.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY