March - April2020
ISSN: 0193-4120 Page No. 6104 - 6113

Fuzzy Logical Method Based Analysis of Safety Data Management and Risk Management In IOT Sector

T.S.Aravinth[1], Mr.E.Arunkumar[2], Dr.C.Vimalarani[3]
[1]Asst Prof,Dept of ECE ,Karpagam Academy of Higher Education,India
[2]Asst Prof,Dept of EIE, Karpagam College of Engineering, India.
[2]Associate Professor, Karpagam Institute of Technology,India
aravinth.ts@kahedu.edu.in

Article Info
Volume 83
Page Number: 6104 - 6113
Publication Issue:
March - April 2020

Article History
ArticleReceived*: 24 July 2019*
Revised*: 12 September 2019*
Accepted*: 15 February 2020*
Publication*: 01 April 2020*

Abstract:
There has lately been much focus on the Internet of Things (IoT) by both organization and instutions A stable and safe IoT connectivity and interaction is necessary for the best functioning of the entire IoT network. A robust IoT network protection can be achieved by facilitating and creating reliable communication between items (nodes). The latest issues such as the absence of clever group -based confidence solutions for networks and the identification of malicious nodes assaults on the IoT trusting infrastructure, like poor service providers.. Furthermore, we are building a pointless, logical approach for the detection of fraudulent nodes engaged in inadequate delivery of services.Ultimately, we create a safe message system to ensure IoT network security that enables reliable node-to-node communications. The message system with a serial communication framework can use that hexadecimal meaning.We have performed detailed tests under different network size variations to evaluate the work of our proposed solutions as well as to monitor the effectiveness of the suggested methods with respect to several types of viral behaviour.

Keywords: *Internet of Things, Fuzzy Logic based approach, Cluster Based Trust*.

1. Introduction

The Iot is a brand new to inventions and research for software and telecommunications networks. It has turned the Internet into communication between people and even collaboration between objects[1]. This has been done through the development of intelligent machines that can determine without human intervention and the exchange of data with other devices to getv a particular goal[2].

Nonetheless, the addition to the public network of all these tools presents different safety problems since most web applications and protocols for interaction have not been developed initially for IoT assistance[3]. such IoT.Standardization via an IoT portal is a well-established approach to solve this control problem[4]. Sadly, new services will be needed. It is scalable and modular platform that has no impact on the efficiency and usability of

Published by: The Mattingly Publishing Co., Inc

March - April2020
ISSN: 0193-4120 Page No. 6104 - 6113

a growing number of devices.It trust protection strategy offers cryptographic security via access control through through confidence levels, but it contributes to increased burden due to time and strngth usage[5]. As its versatility requires additional components, it is easily integrated into utility-based decision-making. In developing a secure mechanism for interaction and exchanging of messages between IoT nodes, a modern solution to fluffy protection protocols and confidence management for Io T-based clusters is introduced utilizing a new IoT safety protocol to cope with these problems.{6,7].

The rest of this paper is structured in the following way: reviews research related to literature. It then includes IoT Node Message System Stable definitions. It gives a summary of beliefs and fluorescent algorithms afterwards. A smart protocol for protection may be provided alongside this. The experiments, tests and analysis are covered.

2. Related Works

Moseniaindicstes the imptovementdure to IoT to multiple communication protocols with transceiver miniaturization providing an Technology advances have Internet connected computer and sensing tools[8].These, however, are at risk of attacks and possible security and privacy risks, particularly if the data is moved from one cluster to another. Although the real challenge of trust management has been argued and accepted as being scalability, a number of strategies to tackle the issue of trust management of IoT have been proposed.Therefore it is important to consider the design of intelligent trust management approaches in the next [9].

In order to create a new hierarchical trust management system for IoT that is based on the supernode. The IoT system needs to evolve in order to establish an effective trust network, developing the nodes that require a trust management protocol.This requires a dynamic system that addresses the threat of hostile and social nodes[10]. Thus their plan focuses on ensuring efficient connectivity is required for each cluster.

The concept is to use a security protection and counterfeiting approach focused on XOR manipulation. In this design, the logic is based on an architecture which concentrates on the interaction between common identifiers and certain resources.Ray has introduced a RFID protocol and to support implementation on the basis that problems can be personalized and scaled..

In Alshehri, an adaptive confidence management clustering strategy for IoT network devices communicating with other nodes.It has software that allows a heterogeneous network interactions with IoT apps and devices with each other. A master node and several groups are expected to handle things central through a network in the hierarchical system. It provides a joint trust system in which networks can communicate in collaboration with each other. The achievement of scalability relies on the positioning of IoT nodes in clusters or groups according to their trust values.

3. Proposed method

This paper focuses primarily on developing an analysis of safety and insightful methods for IoT system management.

To order to identify the security threats encountered, other methods are implemented

Published by: The Mattingly Publishing Co., Inc

March - April2020
ISSN: 0193-4120 Page No. 6104 - 6113

depending on the Fuzzy clustering procedure. Two separate groups such as the Fuzzy method, which reflects the results of security IoT methods, are responsible for the main process.

Several variations in the systemic and parametric variables are addressed in the IoT safety process. It displays the thorough summary analysis in Figure 1. The safety criteria include storage devices, cameras, contact activators, monitoring, finding, detecting and processing techniques, which are known to be the protection specifications..number of elements calculated in the security system estimate those elements for violation, damage, deterioration and exploitation in particular.

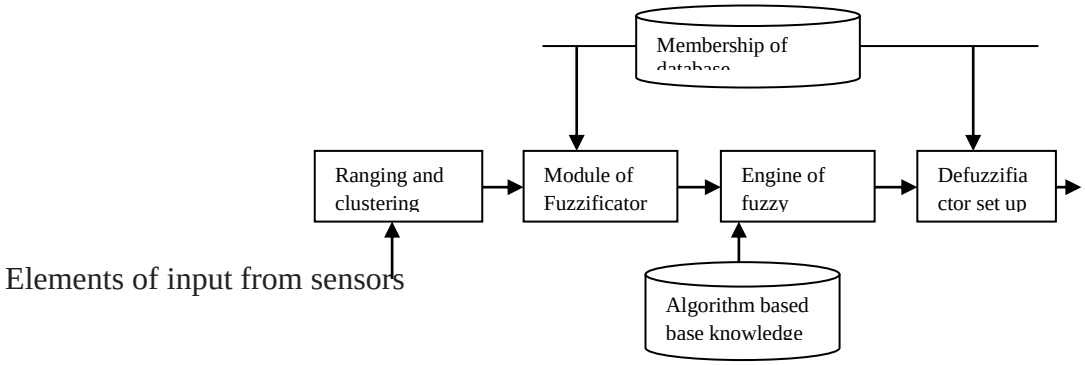

Figure:1 Intelligent agent structure diagram

The interest of the agent intelligent approach is to clearly identify the security risk of traffic input from every IoT component and to to get congestion data from each device. The structural diagram above is well implemented by an interference mechanism and consists of an intelligent agent architecture that get the actual from each device into the network region and clustering.

Both outputs are used to describe the rank and risk of the input to the Fuzzificator module, and here the function is transformed into a fugitive array of equations. The vector is then converted to Fuzzificator module

Finally eventually defuzzifiactor to convert the entire fuzzy output array into a Crisp amount of fluorescent system formulas. Both observation and traffic models based on the anomalous detection actions used by the application-based guidance program are here in depth observed. And then, decisions were made primarily to reduce the hazard protection of IoT components and all information is shared with other agents.

Published by: The Mattingly Publishing Co., Inc

March - April2020
ISSN: 0193-4120 Page No. 6104 - 6113

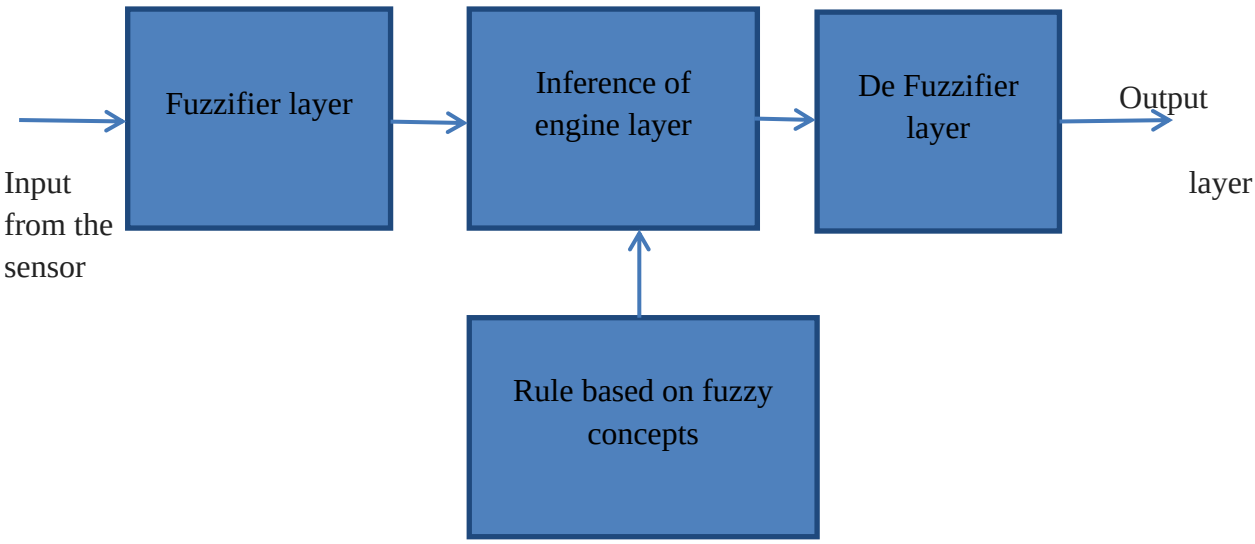

Figure: 2 Fuzzy Architecture Diagram

The sensor outputs are added to the Fuzzifier block in order to lower the sophistication of the system and is transferred to the interference layer engine in which the formulas are translated to vague concepts. It is then transferred to the de Fuzzifier layer and then all security risks are reduced.

The performance analysis and the mean period of likelihood were accompanied by an algorithm to calculate security risk mitigation

$$Q_{ws} = Q\,(p_s \leq P_{fs}) \quad (1)$$

This includes network status elements (p_S), data analysis time (p_I),

decision time-making (p_D), network relevant elements (p_n), network management (p_c) formatting the management execution solutions.

$$p_s = p_s + p_i + p_D + p_n + p_m + p_c \quad (2)$$

The numerical variable hazard is calculated by S, which is defined by a loss by a certain amount of values of potential formulas.

$$S = R_{vbn} * X \quad (3)$$

There, R vbn is the likelihood and X is alluded to as numerical risk to the material function. The safety monitoring risk in the context of IoT is defined here at all levels, and threats and resources are described at all stages.

$$Z \subseteq X,\ AS \subseteq Z \quad (4)$$

The risk numbers can here be indicated as the category value M e and the weighting danger vector F e and the threat times are represented as è click. Equation expression is alluded to as

$$V_e = (M_e * F_e) / \Delta p \quad (5)$$

It produces input data from the decision-making system and reduces the risk of safety of IoT components automatically.

Published by: The Mattingly Publishing Co., Inc

March - April2020
ISSN: 0193-4120 Page No. 6104 - 6113

The probability equations are determined based on the behavioral functions and the equations are followed as

$$Q_i(n) = Q_i^{np}(s) + Q_i^{m}(s) \quad (6)$$

$Q_i^{np}(s)$ determines the evaluated behavioral type of equation and $Q_i^{m}(s)$ quantitative term of equation.

$$Q_i^{M}(n) = \frac{m_i}{M} + (M_e * F_e) / \Delta p \quad (7)$$

As per considering the future interaction of the equations all the nodes and the parameters are calculated as follows

$$Q_i^{M}(n) = U_i^{d,m}(n) + \sum_{n=1}^{N} U\,i\,d,m\,(n)\ \frac{m_i}{M} \quad (8)$$

The previous interactions are denoted as $U_i^{d,m}(n)$ and the integral part of equation is denoted as $\frac{m_i}{M}$.

According to the fuzzification rule the above equation of the output is expressed in the form of de fuzzification module of equations followed as

$$Q_i^{M}(n) = \prod_{i-1}^{n} U_i\,d,m\,(n) + \sum_{n=1}^{N} U_i\,d,m\,(n)\ \frac{m_i}{M} \quad (9)$$

The problem of clustering of the formal finite collection of items is indicated under all items may hereby be identified as Q component descriptive. The cluster range property is observed

$$\bigcup_{j=1}^{d} D_j = Y,\ D_j \cap D_i = \emptyset \quad (10)$$

In order to analyze the distances. The method of decomposition criteria is followed

$$\sum_{j=1}^{d} \sum_{y_{s\in D_j}} (w_j - y_s)^2 \longrightarrow \min \quad (11)$$

Fuzzy cluster equation could be defined as a type of fuzzy element matrix decomposition

$$K(u) = [micro_{sj}] \quad micro_{sj} \in [1, 1] \quad (12)$$

Degree of membership of the third line consisting of vector Y s and the fulfilled condition is followed as cluster equations

$$\sum_{j=1}^{d} = 1,\ 0 < \sum_{s=1}^{n} \mu_{sj} < N \quad (13)$$

Here, the simplest case can then be determined by considering thefuzzy set as follows: the following:

(j=1)^(d):
(14)

the next question: The cluster fuzzy equation of the weight factor cluster can thus be determined: the cluster of fuzzy equations of the weight factor

W j =(μ s = 1)^(n)^(μ s)^(n) (15)

Algorithm: Risk management problem

1. **Procedure:** using base over knowledge system study the algorithm
2. **Input**:S = (r, x) by getting the function of probability of the given input.
3. Begin parameters of the optimization
4. For $(o_j, y_s) \in S$ o
5. Calculate fuzzy grouping.
6. Compute Vparametric setup
7. Calculate PDF J
8. Incrementi(x)

Published by: The Mattingly Publishing Co., Inc

March - April2020
ISSN: 0193-4120 Page No. 6104 - 6113

9. **End f**
10. **Till getting sigmoids**
11. **End**

Risk management question is calculated by the basic knowledge process software and here the likelihood variable is defined for all input functions. The function parameters were configured on the basis of the IoT. The equation is now repeated until the cluster of fluffy equations is obtained. In the algorithm methodology, the estimation defines the parameters of the likelihood variable.

4. Results and Discussion

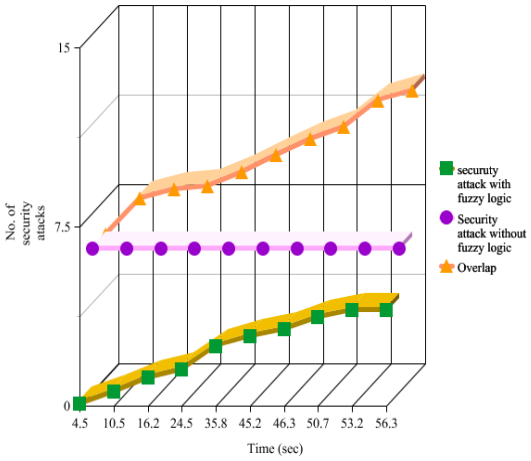

Fig 3 Contrast on - off assaults with and without Fuzzy logic.

Nevertheless, no new on attacks occur after 17s using the fumarous methods proposed in this article. The sum of off attacks continues to fell between 0 and 17 sec. In the case of such threats, the on - off assaults against the orange line indicating [11,12] a steady increase in these attacks will not take place without fuzzy systems. It indicates that this paper's fumigated system senses attacks successfully and can stop the assault after the bootstrap.

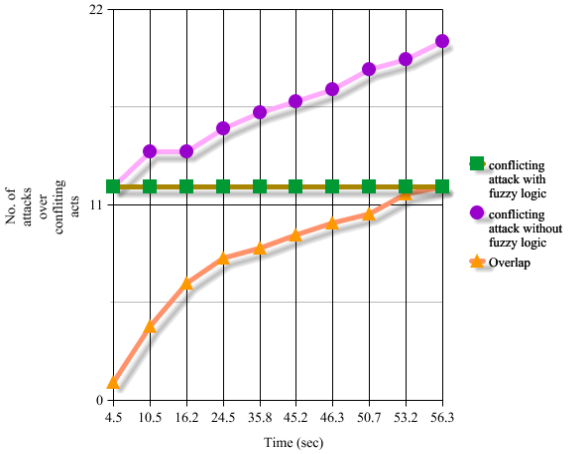

Figure 4: Conflicting attack

Figure 4 Compared to on-off attacks, a conflicting behavior attack node of 30 seconds is calculated using the method suggested. The number of contradictory behavioral attacks with fuzzy strategies after 30 s does not rise, because new attacks do not arise [13,14]. The Red Line, which suggests inconsistent attacks without fluid mechanisms, is still on the rise as the attacks are not blocked. This indicates that it is possible to stop conflicting behavioral attacks with the suggested protocol.

Published by: The Mattingly Publishing Co., Inc

March - April2020
ISSN: 0193-4120 Page No. 6104 - 6113

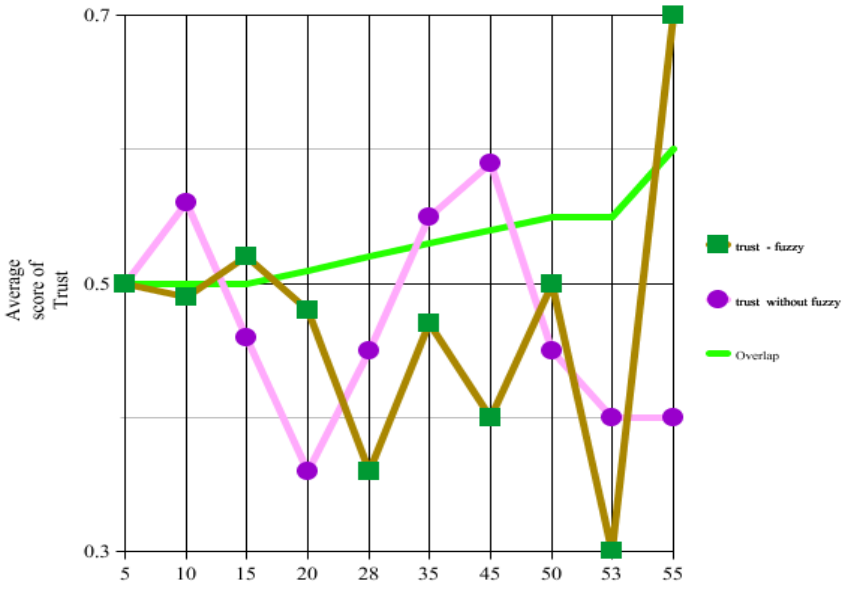

Figure 5: Trust rate

Fig 5 ratings for the testt. Within our system, a node provides a rating which is the basis for the confidence level after receiving a service answer. This score is the service value of the answer the provider receives. Master Node 1 detects dynamic rows and, while Node 7, the bad service supplier, varies, without the blurry structures. It gives the mean quality of service of the whole network improves when a fuzzy function is implemented.[14-19]

In this 100 node situation, fuzzy logic also leads to trust. This figure 6 is the same as the typical. The ifferenceof the value of confidence and the value of a furious faith is that of a trust without fuzzy.The base case requires three hostile nodes with 12 cluster nodes. The proportion of malicious nodes is 50%. However, in 200 group nodes, there are 70 viral nodes. This is 42.5% of the malicious nodes

Published by: The Mattingly Publishing Co., Inc

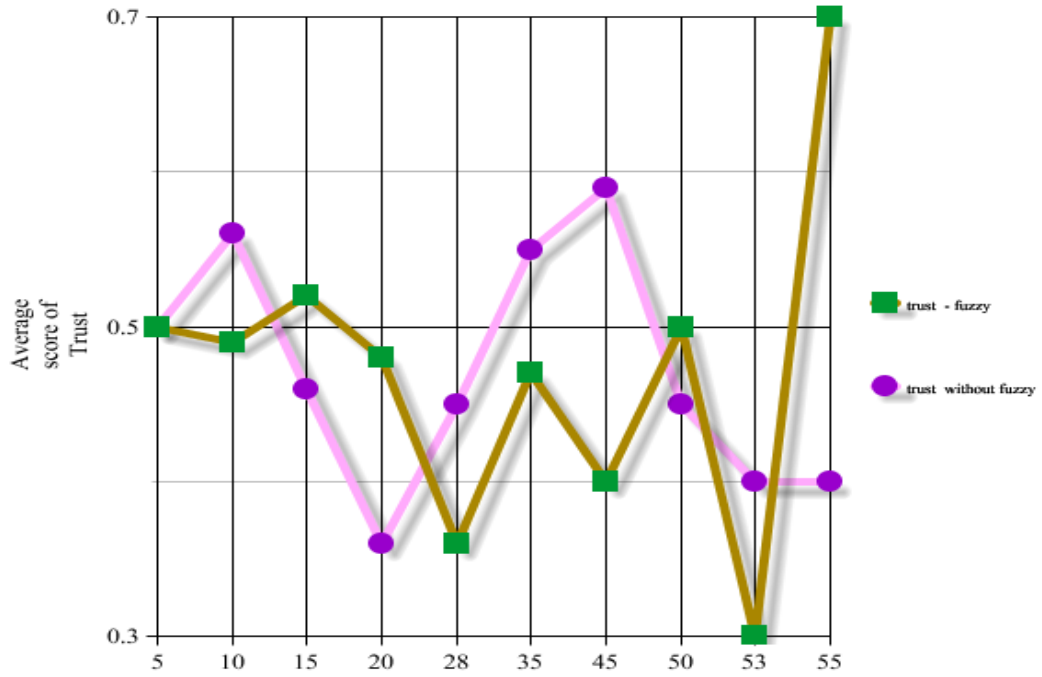

Figure 6: Confidence Quality

5. Conclusion:

Security and trust in IoT nodes is a central, pressing issue and a major focus in contemporary literature. A network can continuously up or down starting to join the network and existing nodes exiting the network. Such improvements in network size should be tailored to a confidence approach. we propose a cluster-based, fluid-logical approach to address this critical problem, which group existing nodes into groups. First, we suggest a protocol utilizing furious reasoning to identify attacks on-off, contradictory attacks on the actions and malicious nodes. Furthermore, we showed how this strategy utilizes useless reasoning to control IoT nodes in order to maintain most of it. Third, a robust IoT node messaging mechanism utilizing serial communication-like hexadecimal values.In order to detect the scalability of our suggested solution, and also evaluate its effectiveness in identification of hostile nodes such as poor service providers, we have carried out thorough testing and analysis on performance under varying networking sizes. From the experimental results, we have identified our method to identify malicious nodes of the network in a set timeframe of 60s. Ultimately, we find that our strategy easily converges the average measured confidence level to the network's actual average trust value.

References

[1] Zhang, Baoquan, Zongfeng Zou, and Mingzheng Liu. "Evaluation on security system of internet of things based on fuzzy-AHP method." *2011 International Conference on E-Business and E-Government (ICEE)*. IEEE, 2011.

[2] Kotenko, Igor, Igor Saenko, and Sergey Ageev. "Countermeasure security risks management in the internet of things based on fuzzy logic inference." In *2015 IEEE Trustcom/BigDataSE/ISPA*, vol. 1, pp. 654-659. IEEE, 2015.

[3] Baskar, S., Dhulipala, V.R.S., Shakeel, P.M., Sridhar, K. P., Kumar, R. Hybrid fuzzy based spearman rank correlation for cranial nerve palsy detection in MIoT environment. Health Technology. (2019). https://doi.org/10.1007/s12553-019-00294-8

[4] Rantos, Konstantinos, George Drosatos, Konstantinos Demertzis, Christos Ilioudis, and Alexandros Papanikolaou. "Blockchain-based Consents Management for Personal Data Processing in the IoT Ecosystem." In *ICETE (2)*, pp. 738-743. 2018.

[5] Xiaohui, Xu. "Study on security problems and key technologies of the internet of things." In *2013 International conference on computational and information sciences*, pp. 407-410. IEEE, 2013.

[6] Guo, Jia, Ray Chen, and Jeffrey JP Tsai. "A survey of trust computation models for service management in internet of things systems." *Computer Communications* 97 (2017): 1-14.

[7] Manogaran, Gunasekaran, Chandu Thota, Daphne Lopez, and Revathi Sundarasekar. "Big data security intelligence for healthcare industry 4.0." In *Cybersecurity for Industry 4.0*, pp. 103-126. Springer, Cham, 2017.

[8] Ly, Pham Thi Minh, Wen-Hsiang Lai, Chiung-Wen Hsu, and Fang-Yin Shih. "Fuzzy AHP analysis of Internet of Things (IoT) in enterprises." *Technological Forecasting and Social Change* 136 (2018): 1-13.

[9] P. Mohamed Shakeel; Tarek E. El. Tobely; Haytham Al-Feel; Gunasekaran Manogaran; S. Baskar., "Neural Network Based Brain Tumor Detection Using Wireless Infrared Imaging Sensor", IEEE Access, 2019, Page(s): 1. 10.1109/ACCESS.2018.2883957

[10] Rantos, Konstantinos, George Drosatos, Konstantinos Demertzis, Christos Ilioudis, Alexandros Papanikolaou, and AntoniosKritsas. "ADvoCATE: A Consent Management Platform for Personal Data Processing in the IoT Using Blockchain Technology." In *International Conference on Security for Information Technology and Communications*, pp. 300-313. Springer, Cham, 2018.

[11] Baskar, S., Periyanayagi, S., Shakeel, P. M., & Dhulipala, V. S. (2019). An Energy persistent Range-dependent Regulated Transmission Communication Model for Vehicular Network Applications. Computer Networks.https://doi.org/10.1016/j.comnet.2019.01.027

[12] Collotta, Mario, and Giovanni Pau. "Bluetooth for Internet of Things: A fuzzy approach to improve power management in smart homes." *Computers & Electrical Engineering* 44 (2015): 137-152.

[13] Sundarasekar, R., Shakeel, P. M., Baskar, S., Kadry, S., Mastorakis, G., Mavromoustakis, C. X., & Vivekananda, G. N. (2019). Adaptive Energy Aware Quality of Service for Reliable Data Transfer in Under Water Acoustic Sensor Networks. IEEE Access.

[14] Mishra, Nilamadhab, Chung-Chih Lin, and Hsien-Tsung Chang. "A cognitive oriented framework for IoT big-data management prospective." In 2014 IEEE International Conference on Communiction Problem-solving, pp. 124-127. IEEE, 2014.

[15] Ravichandran, R., Balachander, K., Amudha, A., Ramkumar, M. S., &Kuppusamy, S. (2017). Estimation Of Electrical Parameter Using Fuzzy Logic Controller Based Induction Motor. *International Journal of Control Theory and Applications*, *10*(38), 205-212.

[16] Veluchamy, R., Balachander, K., Amudha, A., Ramkumar, M. S., &Emayavaramban, G. (2019). ANALYSIS AND ENERGY EFFICIENCY OF SMALL-SCALE WIND ENERGY CONVERSION SYSTEM USING ADAPTIVE NETWORK BASED FUZZY INTERFERENCE SYSTEM (ANFIS) OF MAXIMUM POWER POINT TRACKING METHOD. *Mathematical & Computational Forestry & Natural Resource Sciences*, *11*(1).

[17] Kalimuthu, T., Balachander, K., Amudha, A., Emayavaramban, G., & Ramkumar, M. S.

(2019). AN EFFICIENT HIGH STEP UP CONVERTER FOR AUTOMOBILE APPLICATIONS USING FUZZY LOGIC CONTROL TECHNIQUE. *Mathematical & Computational Forestry & Natural Resource Sciences*, *11*(1).

[18] Shaheeth, M. M., Kavitha, D., Amudha, A., Ramkumar, M. S., Balachander, K., &Emayavaramban, G. (2019). GRID CONNECTED WIND ENERGY CONVERSION SYSTEM WITH UNIFIED POWER QUALITY CONDITIONER (UPQC) BY FUZZY LOGIC. Mathematical & Computational Forestry & Natural Resource Sciences, 11(1).

[19] Shakeel, P. M., Baskar, S., Sampath, R., & Jaber, M. M. (2019). Echocardiography image segmentation using feed forward artificial neural network (FFANN) with fuzzy multi-scale edge detection (FMED). International Journal of Signal and Imaging Systems Engineering, 11(5), 270-278.