International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6, August, 2019

Intrusion Detection in IoT based Smart Networks using Fuzzy Brain Storm Optimization Technique

Suresh B, Venkatachalam M, Saroja M

Abstract*: The Internet of Things (IoT) is characterized as an approach where objects are outfitted with sensors, processors, and actuators which include design of hardware board and development, protocols, web APIs, and software systems, which combined to make an associated architecture of embedded systems. This connected environment enables technologies to get associated with different networks, platforms, and devices, making a web of communication which is reforming the manner in which we communicate with the world digitally. These connected embedded systems are changing behaviour and interactions with our environment, networks, and homes, and also with our own bodies in terms of smart devices. Security and privacy are the most significant consideration in the field of real-world communication and mainly on IoTs. With the evolution of IoT the network layer security in the IoT has drawn greater focus. The security vulnerabilities in the IoT system could make security risks based on any application. Therefore there is an essential requirement for IDS for the IoT based systems for avoiding security attacks based on security vulnerabilities. This paper proposed a fuzzy c-means clustering with brain storm optimization algorithm (FBSO) for IDS based on IoT system. The NSL-KDD dataset is utilized to evaluate and simulate the proposed algorithm. The results demonstrate that the proposed technique efficiently recognize intrusion attacks and decrease the network difficulties.

Keywords*: Internet of Things, Brain Storm Optimization, Intrusion Detection System, Fuzzy C-means clustering, Swarm Intelligence.

I. INTRODUCTION

Development of various technology domains like sensors, automated detection and tracking, embedded processing, broadband Internet connection, wireless transmission, and appropriated facilities has expanded the capability of comprising smart devices into our day by day work over the Internet. The intersection of the smart devices and Internet which can interact and communicate with one another characterizes the IoT. This new model is perceived as a standout amongst the very significant in the Information and Communication Technology (ICT) industry for the following years. As indicated by Gartner Inc., by 2020 the IoT might have 26 billion units. Cisco Systems anticipated which the IoT will make $ 14.4 trillion because of the integration of expanded incomes and low expenses for organizations from 2013- 2022 [1]. IoT relates to the basic thought of things, particularly regular devices which are accessible, detectable, addressable, locatable, over data sensing devices as well as controllable by means of the Internet, regardless of the communication implies (by means of RFID, wireless LAN, WAN, or different methods). IoT is an internet of three things: (1). Human to Human, (2) Human to machine/things, (3) Things/machine to things/machine, communication over the internet [4].

IoT devices are fixed with a group of sensors while likewise offering the way to develop a network connection, empowering the communication of the gathered data to a wireless node. IoT stands the network of vehicles, physical devices, structures and different things integrated with sensors, actuators, electronics, software and connectivity of network which enable these items to accumulate and communicate information. The word internet refers a distributed network and objects in the IoT sense could implies to the broad assortment of devices like electric clams in coastal waters, biochip transponder on farm animals, cars with internal sensors and heart monitoring implants. The IoT provides a broad assortment of smart devices all of which face the complexity of verifying total security. As the devices are for the most part so different in their heterogenic condition is often used as an optional and manufacture and owners alike to avoid adequate security controls. While the IoT will make life simpler, there are noteworthy security challenges in its utilization. Slow advancement and restricted commercialization have driven some industry observers to hop to call it as "Internet of No Things". At that point last the innovative developments caused it to defeat this name. Commonly it's confronting a lot of security issues it's presently called as "Internet of Insecure Things". Your information may be taken care of by an attack without safety efforts set up. Attackers could complete three various tasks, for example, task control, steal data and disrupt services [2].

Revised Manuscript Received on October 30, 2019.
* Correspondence Author
Suresh B*, Research Scholar, Department of Electronics, Erode Arts and Science College (Autonomous), Erode, Tamilnadu, India. and Assistant Professor, Department of Electronics and Communication Systems, VLB Janakiammal College of Arts and Science College (Autonomous), Coimbatore, Tamilnadu, India.
M.Venkatachalam, Associate Professor and Head, Department of Electronics, Erode Arts and Science College (Autonomous), Erode, Tamilnadu, India.
M.Saroja, Associate Professor, Erode Arts and Science College (Autonomous), Erode, Tamilnadu, India.

The three-layer architecture is an exceptionally fundamental design and satisfies the fundamental concept of IoT. It was developed in the beginning phases of improvement of IoT. The 3-layer architecture was the fundamental architecture. Because of constant advancement in IoT, it could not satisfy every necessities of IoT.

In this way, researchers propose architecture with 4 layers. It has 3 layers like the past architecture, yet it likewise has another layer known as support layer. The four-layer architecture assumed a significant part in the advancement of IoT. There were likewise a few difficulties in terms of storage and security in 4-layer architecture. Researchers proposed architecture with 5-layer to develop the IoT safe. It has 3 layers like past architecture whose names are application layer, transport layer, and perception layer. It additionally contains two additional layers. These new layers are business layer and processing layer. It is viewed as that the new proposed architecture can satisfy the prerequisites of IoT. It additionally can make the applications of IoT secured.

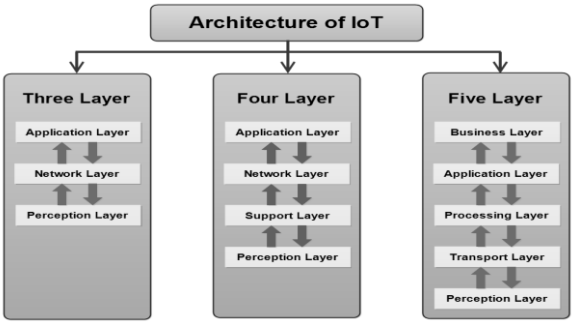

Figure.1. Evolution of IoT Architectures [3]

1.1 IDS

Intrusion is a pointless or malignant action that is hazardous to nodes of sensor. IDS are utilized to monitor the network's malignant traffic. It could perform as a second path of the barrier that could safeguard the network out of intruders. IDS could be a hardware or software tool. IDS could analyze and examine systems and user activities, identify signatures of familiar assaults and classify malignant network actions. The objective of IDS was to track the nodes and networks, identify different network interruption, and indicate the users about interruption. The IDS functions as an alert or spectator of network, it ignores damages of the system by producing an indication previously the aggressors start an attack. It could identify the external and internal attacks. The internal attacks were started withcompromised or malignant nodes which were the network segment during external attacks were propelled by outsiders who were started through the external network. The IDS identify the packets of network and decide if they were genuine usersor intruders. Three features of intrusion detection comprise: Monitoring, Analysis, Alarm and detection. The observing segment observes the traffics of network, resources and patterns. Detection and Analysis was a center module of intrusion detection that identifies the interruption as indicated by the predetermined algorithm. Alert section generates an alert if an intrusion is identified [3].

IDSs are assorted as Network-based (NIDS) and Host-based (HIDS)IDS. NIDS interfaces with at least one or more network sections and observes traffic of network for malignant actions. HIDS is connected to a computer and observes malignant actions happening inside the system. In contrast with NIDS, the HIDS analyzes not just network traffic as well as changes in file system, system calls; inter process communication, running processes, and application logs [1].

IDS are a security system that performs essentially in the IoT system's network layer. IDS implemented for an IoT framework must have the option to investigate packets of information and produce responses continuously, determine packets of data in various IoT layers connect through various stacks of protocol, and adjust to various innovations in the IoT system. The IDS are intended to IoT related smart systems must work under restrictive states of less capacity of processing, quick response, large size information processing. In this manner, regular IDS might not be completely appropriate for IoT systems. Security of IoT is a consistent and major problem; along these, a recent comprehension of the vulnerabilities of security of IoT frameworks and advancement of relating moderation methodologies were needed [5].

II. Related Works

Bruno B Z, et al., (2017) proposed a review about IDS analysis for IoT. They chose 18 articles in the literature which presented particular IDS plans toIoT or designed attack identification techniques for IoT which could be a segment of IDS. These articles were proposed in the year range of 2009 and 2016. They presented taxonomy to classify the articles that depended on the accompanying qualities: identification technique, IDS placement technique, validation method and security risk. They acquired which the analysis of IDS models for IoT was as yet beginning.

Sarika C and Nishtha K, (2019) proposed this article by concluding a study on the IDS against different attacks dependent on 6LoWPAN and RPL explicitly for IoT condition. They described about lot of security attacks done on IoT network and the mitigation techniques yet at the same time numerous attacks have not been assessed at this point. Thus, several researches were expected to moderate these attacks. Mohamed F E, et al., (2018) presented a complete review of the most recent IDSs intended for the IoT system, with an attention on the comparing techniques, features and systems. This work likewise provided profound knowledge into the IoT design, evolving security limitations, and its connection to the IoT architecture layers. This research exhibited that in spite of past analysis with respect to the design and execution of IDSs for the IoT model, creating proficient, dependable and solid IDSs for IoT-based smart conditions was as yet a critical undertaking. Key contemplations to the advancement of such IDS were presented as a future viewpoint in the conclusion this study.
Suganthi and Usha, (2018) proposed a total review about the taxonomy, summarized and composed recent research results of the IDS in IoT.

Through this analysis, the authors were easy to distinguish the security loopholes emerging out of the data exchange technologies in the Internet of Things and furthermore get familiar with the different security attacks and attempts to deal with alleviate those attacks.

Rabie A. Ramadan, (2017) presented a new Brain Storming Optimization Algorithm. The proposed algorithm utilized Fuzzy C-mean rather than K-mean in the clustering stage. Likewise, the proposed new BSO algorithm relied upon the predator/prey to escape the local optima. Also, the issue of Energy Topology Control in WSNs was comprehended by BSO and FBSO. Based on their verification of concept analysis, FBSO results appeared to be successful and outperformed the initial version of BSO.

III. PROPOSED METHODOLOGY

3.1 BSO

The BSO is another sort of SI algorithm that depends on collective behaviour of the human, which is, the brainstorming procedure. It accepts the Brain Storming method that humans use. Individuals meet up thinking about a solution or more to an issue. They build up their concepts, share them, assess them, select the best concepts, after go for iterations. The brainstorming process goes for iterations to achieve a proficient solution for the issue close by through cooperation between individuals that are firmly related or not to the issue. This procedure demonstrated to be effective in consideration of real-life complex issues.

In 2011, Yuhui Shi configured this technique for solving the optimization issues in various fields of science. The author considered the human as the most intelligent animal and adjusting his/her perspective should result effective solutions. As per Yuhui, two iterations brainstorming procedure partitioned into 8 steps condensed below. As can be seen, step 6 performs as a divergence to the human from getting trapped in similar concepts. This procedure is converted into formal algorithmic procedures to be reasonable for optimization issues including generation process, clustering process, mutation and selector operators. The real BSO utilizes K-Mean as the clustering method.

Brain Storming Process:

Step.1: Get individuals from various backgrounds as much as possible.

Step.2: Individual must produce many concepts according to the following rules:

Rule.1: Suspend Judgment

Rule.2: Anything Goes

Rule.3: Cross-fertilize (Piggyback)

Rule.4: Go for Quantity

Step.3: Some individuals would be selected to be the owners of the issue to select the good concepts from the gathered individuals.

Step.4: The selected concepts would be utilized as base for producing more concepts according to the similar rules indicated in step 2.

Step.5: Repeat Step 3 to select the good generated concepts;

Step.6: In any order select an object and utilize the tasks and aspect of the object as clues, produce additional concepts based on the rules;

Step.7: Let the users select many better concepts;

Step.8: By this step, we hope that good concepts are reached to be treated as a key to the problem in hand.

Gaussian random values were combined to produce new individuals based on equation (1).

$$X_{new}=X_{old}+\varepsilon*(\mu,\sigma) \quad (1)$$

Where,*new*- recently produced individual and *Xold*- selected individual to produce new one. (μ,)- Gaussian functions with variance σ and mean μ. ε- contribution weight of Gaussian random value and calculated by equation (2).

$$\varepsilon=logsig\left(\frac{0.5*m_{iteration}-c_{iteration}}{k}\right)*() \quad (2)$$

Where, logsig() is the logarithmic sigmoid function, $m_{iteration}$- maximum count of iterations, $c_{iteration}$- current iteration value, *k*- constant for modifying the logarithmic sigmoid function slope, and rand()- random generator function that produces a number among 0 and 1.

3.2 Fuzzy C-Mean Clustering

FCM clustering is initially presented by Enrique, 1970. Fuzzy C-mean has been utilized in clustering, pattern detection, image processing and numerous different issues. The concept behind FCM is the fuzziness of effects every component in the information to various groups. Unlike the K-Mean algorithm where every component has a place just with a specific group, FCM relaxes this hard limitation to enable every component to have a place with numerous groups with a membership degree subject to the summation of all the membership degrees of each point to every cluster must be one. FCM utilizes a minimization function to segment the points or the datasets. In this way, the membership function U may have components among 0 and 1 with a summation of a data point is equivalent to 1 as given in condition (3).

$$\sum_{i=1}^{c} u_{ij} = 1, \forall_j = 1, \dots \dots, n \quad (4)$$

The objective/cost function is written as follows:

$$j(U, c_1, \dots \dots, c_c) = \sum_{i=1}^{c} J_i = \sum_{i=1}^{c} \sum_{j=1}^{n} u_{ij}{}^{m} d_{ij}{}^{2} \quad (5)$$

Where uijvalue is in a range of [0, 1], *c*i is the center of a cluster i, dij- Euclidian distance among the *c*i- cluster center and the j- data point, and m- weight exponent and its value is the range of (1, ∞). However, the constraints of *c*i and uij to reach the required minimum are as follows:

$$c_i = \frac{\sum_{j=1}^{n} u_{ij}^{m} x_j}{\sum_{j=1}^{n} u_{ij}^{m}} \quad (6)$$

$$u_{ij} = \frac{1}{\sum_{k=1}^{c} \left(\frac{d_{ij}}{d_{kj}}\right)^{2/(m-1)}} \quad (7)$$

Hence, FCM begins by initializing U as a membership matrix by random values satisfying equation (3). The fuzzy cluster centers c is then calculated utilizing equation (5). The cost function is then computing utilizing equation (4) and depends on its value the algorithm may stop, whether it is under certain value or the improvement from the past iteration is less than specific threshold. If there is a way for improvement, U is then evaluated utilizing equation (6) and the algorithm is repeated again.

3.3 Fuzzy Brain Strom Optimization Algorithm

In this section, our proposed FBSO is presented. As can be seen from the previous sections, BSO depends mainly on the clustering and the algorithm K-mean clustering is used for this reason. K-mean clustering allows each idea to belong to only one cluster and the new cluster center is chosen based on the new cluster members/ideas. In BSO, the generated cluster center concept was treated with higher probability than different ideas in the cluster. Therefore, the global information of the work space is not fully utilized. Consequently, some of the good ideas might be lost due to the focus on the clusters centers [13 – 22].

KDDCUP99 and NSL-KDD were the regularly utilized data sets in IDS research. We utilized NSL-KDD dataset that was accessible in csv form to evaluate and validate the model. The dataset makes out of the attacks appeared in Table.1 and detected as a main attack in IoT system. As per the study of KDDCUP9, its latest form, NSL-KDD, malignant attacks in the NIDS could be characterized into the accompanying four primary classifications:

DoS: when an intruder hinders genuine users' gateway to the provided system or service.

Probe: when an intruder tries to just know data about objective network over host and network scanning actions.

User to Root (U2R): while an aggressor tries to increase a constrained users' benefit to root access or super user (for example through stolen credentials or malware).

Remote to Local (R2L): when an aggressor increases access of remote to a target system reflecting present local users.

Table.1. Types of attacks in NSL-KDD dataset

Types of attacks	Sub Class (Attacks)	New Sub Class (Attacks)
DoS	Back, Neptune, land, Smurf, teardrop, pod	Mailbomb, Apache2, Process table
Probe	Imap, multhop, spy, phf, warezclient, ftp write, warezmaster, guess passwd	Mscan, Saint
U2R	Buffer overflow, load module, perl, Rootkit	Httptunnel, Xterm, Sqlattack, Ps
R2L	Ipsweep, portsweep, nmap, satan	Sendmail, Snmpgetattack, Named, Xsnoop, Snmp guess, Xlock, Worm

Hence the test set includes 17 new attacks excluded in the training set, we could assess the efficiency of the proposed technique in distinguishing obscure or exceptional assaults. The first dataset comprises records of 125,973 of train and records of 22,544 for the test, all through 41 features, for example, source bytes, protocol, signal, features, duration, destination bytes, and so forth. The traffic dispersion of dataset NSL-KDD has appeared in Table.2. At last, we utilize DoS, Probe, R2L, U2R attacks as intrusion attacks and training sets separately.

Table.2. NSL-KDD dataset's Traffic Distribution

Traffic	Training	Test
Normal	64378	9821
DoS	42759	7854
Probe	15616	2452
R2L	985	2142
U2R	50	188
Total	123788	22457

$$Acc = \frac{TP+TN}{TP+TN+FP+FN} \quad (8)$$

$$FAR = \frac{FP}{TN+FP} \quad (9)$$

$$Precision = \frac{TP}{TP+FP} \quad (10)$$

$$Recall = \frac{TP}{(TP+FN)} \quad (11)$$

Accuracy was the level of true identification through every information cases;

False alarm rate describes proportion of misclassified typical examples; Recall indicates how many of the attacks do the model return. Precision portrays how many of the returned attacks are right; TP: true positive, FP: false positive, FN: false negative, TN: true negative.

Table.3. Results of Traffic Distribution of the dataset NSL-KDD with proposed method

Attacks	ACC	FAR	Precision	Recall
DoS	97.22	0.9	97.12	97.70
Probe	96.89	0.8	97.37	96.40
R2L	95.41	7.6	91.75	93.21
U2R	95.68	1.9	96.20	96.97

Table.3 represents the traffic distribution of the NSL-KDD dataset performed in terms of accuracy, FAR, precision and recall by using the proposed FBSO method and the related graphical plot is shown in figure.2.

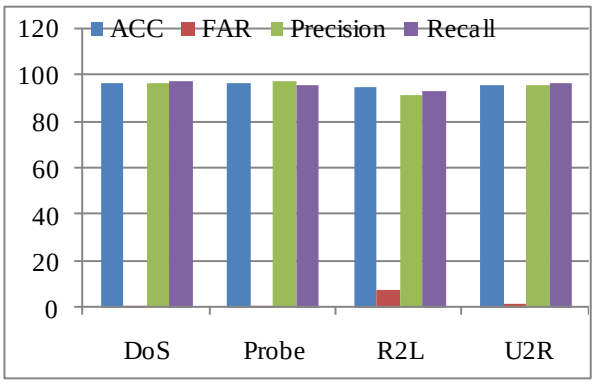

Figure.2. Graphical Representation of Traffic Distribution of the dataset with proposed method

Table.4.Comparison of classification accuracy of the proposed method

Method	DoS	R2L	Probe	U2R
TANN	90.94	80.53	94.89	60.00
BPNN	80.35	89.12	89.12	25.58
FC-ANN	96.70	93.18	48.12	83.33
FBSO (proposed)	97.22	93.51	95.00	90.27

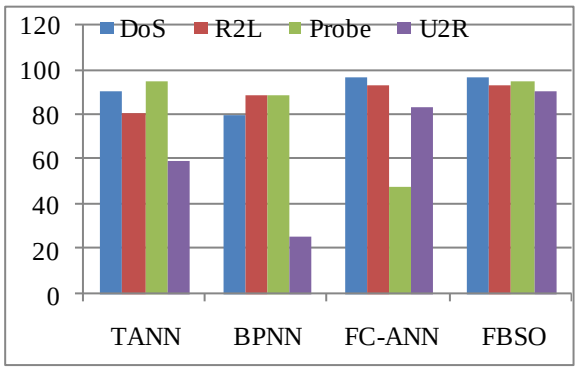

Figure.3. Graphical Representation of Classification accuracy of proposed method with existing methods

Table.4 represents the classification accuracies of the existing methods and the proposed method based on the types of attacks in the dataset like Dos, R2L, Probe and U2R and the figure.3 demonstrates the graphical plot of the classification accuracies.

IV. CONCLUSION

BSO can efficiently process high dimensional and complex data, and the results of the classification are great. So in this work, the Fuzzy C-means with Brain Storming Optimization algorithm is proposed, fuzzy plays out several iterations to provide an optimal structure of network, BSO hence utilizes the acquired structure of the network as IDS system to attacks classification. Along these, confronting various attacks, the issue of how to choose a suitable network structure when utilizing optimization method for intrusion detection is settled, and in this manner, it enhances the classification accuracies and speculation of the system and decreases difficulties of structure of the network. Moreover, the algorithm with fuzzy and BSO model not exclusively could be utilized in detecting intrusion in the IoT yet, in addition, could be implemented to different conditions, for example, classifications and detection. For various sets of training, an optimal structure of network is properly created for classifications. In addition, for limited training sets, high accuracies of classification could likewise be accomplished, that discovers attacks with low-frequency in IDS. We considered to use different classifier to overcome the training and computational time and to increase the classification accuracy in future.

REFERENCES

1. Bruno Bogaz Zarpelão, Rodrigo Sanches Miani, Cláudio Toshio Kawakani, and Sean Carlisto de Alvarenga, 2017, A Survey of Intrusion Detection in Internet of Things, Journal of Network and Computer Applications, http://dx.doi.org/10.1016/j.jnca.2017.02.009
2. Vaishnavi S and Sethukkarasi.R, 2017, Various Types of Attacks and Its Detection Algorithm in Internet of Things (IoT): Survey, Proceedings of International Conference on Advances in Science, Management and Engineering.
3. Sarika Choudhary and Nishtha Kesswani, 2019, A Survey: Intrusion Detection Techniques for Internet of Things, International Journal of Information Security and Privacy, Volume-13, Issue-1.
4. Keyur K Patel and Sunil M Patel, 2016, Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges, International Journal of Engineering Science and Computing, Volume 6, Issue No. 5.
5. Mohamed Faisal Elrawy, Ali Ismail Awad, and Hesham F. A. Hamed, 2018, Intrusion detection systems for IoT-based smart environments: a survey, Journal of Cloud Computing: Advances, Systems and Applications, 7:21.
6. Leonel Santos, Carlos Rabadão, and Ramiro Gonçalves, 2018, Intrusion Detection Systems in Internet of Things, IEEE, pp-1-7.
7. Somayye Hajiheidari, Karzan Wakil, Maryam Badri, and Nima Jafari Navimipour, 2019, Intrusion detection systems in the Internet of things: A comprehensive investigation, Computer Networks (2019), doi: https://doi.org/10.1016/j.comnet.2019.05.014.
8. Tariqahmad Sherasiya and HardikUpadhyay, 2016, Intrusion Detection System for Internet of Things, IJARIIE, Vol-2, Issue-3.
9. S. Suganthi and D.Usha, 2018, ASurvey of Intrusion Detection System in IoT Devices, IJAR, Int. J. Adv. Res. 6(6), 23-30.
10. Shi Cheng, Quande Qin, Junfeng Chen, and Yuhui Shi, 2016, Brain storm optimization algorithm: a review, Artif Intell Rev, Springer, DOI 10.1007/s10462-016-9471-0
11. Rabie A. Ramadan, 2017, Fuzzy Brain Storming Optimization (FBSO) Algorithm, Int. J. Intelligent Engineering Informatics, Vol. 10, No. 150.
12. Shi Cheng, Yifei Sun, Junfeng Chen, Quande Qin, Xianghua Chu, Xiujuan Lei and Yuhui Shi, 2017, A Comprehensive Survey of Brain Storm Optimization Algorithms, IEEE, pp-1637-1644.
13. Muhammad Burhan, Rana Asif Rehman, Bilal Khan, and Byung-Seo Kim, 2018, IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey, Sensors, MPDI journal, pp-1-37.
14. Rajendran T & Sridhar K P, 2018, Epileptic seizure classification using feed forward neural network based on parametric features. International Journal of Pharmaceutical Research, 10(4): 189-196.
15. Hariraj V, Khairunizam W, Vikneswaran V, Ibrahim Z, Shahriman A B, Razlan Z M, Rajendran T, Sathiyasheelan R, 2018, Fuzzy multi-layer SVM classification of breast cancer mammogram images. International Journal of Mechanical Engineering and Technology, 9(8): 1281-1299.
16. Muthu F, Aravinth T S & Rajendran T, 2017, Design of CMOS 8-bit parallel adder energy efficient structure using SR-CPL logic style, Pakistan Journal of Biotechnology, 14(Special Issue II): 257-260.
17. Yuvaraj P, Rajendran T & Subramaniam K, 2017, Design of 4-bit multiplexer using Sub-Threshold Adiabatic Logic (STAL), Pakistan Journal of Biotechnology, 14(Special Issue II): 261-264.
18. Keerthivasan S, Mahendrababu G R & Rajendran T, 2017, Design of low intricate 10-bit current steering digital to analog converter circuitry using full swing GDI, Pakistan Journal of Biotechnology, 14(Special Issue II): 204-208.
19. Vijayakumar P, Rajendran T & Mahendrababu G R, 2017, Efficient implementation of decoder using modified soft decoding algorithm in Golay (24,12) code, Pakistan Journal of Biotechnology, 14(Special Issue II): 200-203.
20. Rajendran T & Sridhar K P, 2019, Epileptic Seizure-Classification using Probabilistic Neural Network based on Parametric Features, Journal of International Pharmaceutical Research 46(1): 209-216.
21. Rajendran T, et al., 2019, Recent Innovations in Soft Computing Applications, Current Signal Transduction Therapy, (Article in Press).
22. Emayavaramban G, et. al., 2019, Identifying User Suitability in sEMG Based Hand Prosthesis Using Neural Networks, Current Signal Transduction Therapy, DOI: 10.2174/1574362413666180604100542 (Article in Press).

23. Rajendran T & Sridhar K P, 2019, An Overview of EEG Seizure Detection Units and Identifying their Complexity- A Review, Current Signal Transduction Therapy, DOI: 10.2174/1574362413666181030103616 (Article in Press).

AUTHOR PROFILE

Mr.B.Suresh has completed his B.Sc., M.Sc., M.Phil., and Pursing Ph.D., from Erode Arts and Science College (Autonomous), Erode. Affiliated to Bharathiar University. He has published more than 10 articles in National Journals, International Journals, and conference Proceedings. Presently he is serving as Assistant professor in the Department of ECS, VLB Janakiammal College of Arts and Science College (Autonomous), Coimbatore. His research interests are Microprocessors, Embedded systems and IoT.

Dr.M.Venkatachalam has completed his B.Sc., M.Sc., M.Phil., and Ph.D., degrees from Bharathiar University. He has published more than 100 articles in National Journals, International Journals, and conference Proceedings. Presently he is serving as Associate professor and Head in the Department of Electronics, Erode Arts and Science College (Autonomous), Erode. He has served as principal investigators for many funded projects and guided many scholars leading to the award of Ph.D. His research interests are Thin Film Technology, Microprocessors, Embedded systems and IoT.

Dr.M.Saroja has completed her B.Sc., M.Sc., M.Phil., and Ph.D., degrees from Bharathiar University. She has published more than 100 articles in National Journals, International Journals, and conference Proceedings. Presently she is serving as Associate professor in the Department of Electronics, Erode Arts and Science College (Autonomous), Erode. Her research interests are Thin Film Technology, Microprocessors, Embedded systems and IoT.