JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 2, 2022, p. 2749 - 2757
https://publishoa.com
ISSN: 1309-3452

Implementation of Naive Bayes Classifier for Reducing DDoS Attacks in IoT Networks

Vanlalruata Hnamte[1]
Assistant professor,
Department of Mathematics and Computer Science,
Mizoram University,
Tanhril, Aizawl
Mizoram, India
vanlalruata.hnamte@gmail.com

G.Balram[2]
Assistant professor,
Department of Computer Science and Engineering,
Anurag university,
hyderbad
balaramcse@anurag.edu.in

Priyanka.V[3]
Assistant professor
Department of CSE
Rathinam Technical Campus.
Eachanari,
Coimbatore-641021
priyanka.cse@rathinam.in

Dr. K. V. Nagendra[4]
Professor,
Department of Computer Science and Engineering
GN University.
Hyderabad
drkvnagendra@gmail.com

Naveen P[5]
Assistant professor,
Department of Computer Science and Engineering,
st.joseph's college of engineering,
Chennai,
Tamilnadu,india,
navee4@gmail.com

ABSTRACT

One of the objectives of intelligent devices is to enhance human well-being in terms of convenience and efficiency. Using the Internet of Things (IoT) paradigm, smart environments may now be created. Privacy and security are major concerns in any IoT-based smart real-world setting. There are security dangers to smart environment applications due to IoT-based systems' vulnerabilities. IoT-specific intrusion detection systems (IDSs) are urgently needed to protect against attacks that leverage some of these security flaws. Intrusion Detection Systems (IDS) have played a significant role in network and information system security for more than two decades. Because of its unique properties, such as low-resource devices, specialised protocol stacks, and standardized communication protocols, it is difficult to apply classic IDS techniques to IoT. For the Internet of Things, standard intrusion detection systems suffer from a number of limitations that can be mitigated by combining machine learning technology with them. The purpose of this work is to explain how classic statistical approaches may be used to examine scope distribution diversity in order to choose and optimize features. The Correlation Coefficient approach is used to select the best features for the development of the classifier in this work's "Distributed Diverse Technique of Feature Optimization to Prevent Intrusion Activities on IoT Networks." To train our Naive Bayes classifier, we employed proposal-selected feature sets. There was a decrease in false alarms as well as an increase in classification accuracy.

Keywords- Intrusion detection Systems; IoT; Naïve Bayes, Similarity Coefficient.

I. INTRODUCTION

Electronic applications and services are now so commonplace that enormous breakthroughs in communication systems and the rise of the notion of the Internet of Things have occurred as a result (IoT). Things, or "things," are devices that can detect their environment, connect to one other, and exchange data via the Internet in a developing communications paradigm known as the Internet of Things (IoT). IoT networks are expected to connect one billion IP addresses or items to the Internet by 2022 [1].

There has been recent usage of the IoT paradigm in creating smart surroundings, such as intelligent cities and intelligent homes, with a variety of application areas and related services. By addressing issues relating to the building design, energy usage, and industrial demands, smart environments seek to improve human productivity and well-being [2]. The rapid expansion of Internet-of-Things (IoT)-based services and applications over a variety of networks reflects this objective. There are many examples of smart cities that are based on IoT systems, such as Verona Urban Development in Italy [3].

Sensors in a smart environment work together to carry out tasks. Smart surroundings are being expanded with the use of wireless sensors, wire-less communication systems, and IPv6. Smart cities, smart homes, smart healthcare, and smart services are all examples of such environments. Smart items are more effective when they are integrated with IoT systems and smart settings. Denial-of-service (DoS) and disseminated denial-of-service (DDoS) attacks are two common types of security threats that can affect IoT devices. An IoT network's IoT services and smart surroundings applications can suffer significant damage as a result of such attacks [21].

As a result, protecting Internet of Things (IoT) devices has become a top priority [4]. When a number of DDoS attacks were conducted throughout the US on Friday, October 21, 2016, exploiting the security weaknesses in IoT systems, [5]. Several Internet of Things (IoT) devices and websites were the targets of these attacks. In an IoT network, a monitoring system (IDS) is used to protect the system from external threats. There should be a way to examine data packets in multiple layers of the IoT network with varied protocol stacks and adaptable to various technologies inside the IoT environment with an IDS installed for an IoT system [6]. Low-processing capability, fast response time and high-volume data processing are all critical requirements for an IDS developed for smart settings based on the Internet of Things. Conventional intrusion detection systems (IDSs) may not be enough for IoT contexts. Since IoT security is a constant and critical concern, the development of appropriate mitigation strategies is necessary [20].

It is the goal of this study to develop a practical solution to the network security concerns posed by the Internet of Things. This study's findings will be put to use in the creation of an intrusion prevention system that is capable of detecting Iot devices attacks that are dynamic and sophisticated, as well as intelligently responding to unexpected incursions. As a part of the research, it is also hoped that the algorithm would be improved in terms of variable value and learning rate. The goal of this study is to develop an IoT device intrusion detection system that is more effective. IoT devices will be the subject of this research, which will look at the dangers they provide, the disadvantages of current IDS for IoT devices, and usable technology that may be required to enhance IDS for IoT devices[19].

The network layer is said to be the most common entry point for attackers, according to research. That's why this new intrusion prevention system will concentrate on protocols at the network and transport layers. For the Internet of Things (IoT), the Tcp has recently gained popularity [7]. In this work, the transport layer protocol (TCP) is examined in depth because of its importance. The next sections go through the various ways for detecting and simulating intrusions[18][20].

II. RELATED WORK

Here, we take a look at some of the work being done to address IoT security concerns using new and old machine learning algorithms. The so-called "Systematic Literature Review" was used to compile the works included in this study (SLR). SLR approach can be used to identify, analyse, and interpret works meaningfully. To the greatest extent possible, the method should be open and reproducible [15][16].

prakash et al. [21] conducted a poll that revealed the IoT's strengths and weaknesses. Detecting and retaining proof of an assault or malicious behaviour is critical to a successful IoT network, according to the authors. The study's major goal was to show the serious problems associated with the Internet of Things. Because IoT systems are intended to operate discreetly and independently, the authors admit that detecting their presence is a difficult task. Machine learning has become increasingly significant in recent years to help with security and identification in IoT contexts [9, 10]. However, we haven't come across many examples of machine learning being used in the context of IoT-based security challenges. In recent years, deep learning has received a lot of attention. There are several uses for pattern classification, image analysis, and text mining in network intrusion detection at this time[17][12][23][24].

With encouraging results, Diro & Chilamkurti [24] looked at machine learning as a new intrusion detection method for IoT devices. According to the authors, the addition of additional protocols, primarily from IoT, has resulted in hundreds of zero-day attacks, and most of them are modest versions of previously network-resistant assaults. Network Security Metrics (NSMs) have been examined in depth in this survey, focusing on the Standard Consider Factors System (CVSS) architecture, which is utilised as an input to several security metric models in this survey. The aspects of risk management field has also been compared to other related fields. Primary metric suggestions were thoroughly reviewed in this work, with an emphasis on model-based quantitative NSMs; a comprehensive and thorough evaluation of the other main metric recommendations was also provided. For each piece of work, the advantages and cons are also listed. An in-depth examination of all aspects of the evaluated security metrics, as well as open issues and recommendations for future research, was provided, followed by the discussion of prior work. We can reasonably conclude that the field of model-based qualitative NSMs is still in its infancy and that significant progress still needs to be made, given the evidence presented in this review[22].

Additional security indicators, such as those provided by Granjal et al. [25], could also be useful to users of other Web infrastructures, such as computing and the internet of Things (IoT).

According to Al-Fuqaha et al [26], obstacles and issues related to IoT implementations, and the interplay between big data analytics, cloud computing, and fog computing, were reviewed in their paper. For improved horizontal integration of IoT services, a new intelligent technique for autonomously management, received data, and protocol adaptation was presented. Instead, they focused on IoT protocol and standard development by examining the many protocols and patterns found within IoT environments at various layers, then analysing the protocols themselves to determine their core functioning and intended use. Data analytics techniques and tools for IoT big data are needed, such as the ability to reduce the quantity of inputs, according to the authors, who also studied the consequences of IoT, such as Big Data, clouds and fog computing. We ended with a look at three real-world use cases to show how the various protocols discussed in this survey might be combined to create innovative IoT services that offer new features to end customers [23].

For an IoT network, Lopez-Martin et al. [27] introduced a new network - based intrusion detection approach. Based on a CVAE, the proposed technique incorporates intrusion la- bels into the decoder layers of the CVAE. IoT networks in particular benefit from the proposed model's ability to do feature reconstruction as well as its ability to be used in the current Network Intrusion Detection (NIDS). The proposed method only requires one training phase, hence reducing the amount of time and effort required to implement it[24].

Although Fu et al. suggested that IoT will be a potential aspect of 5G networks, many security procedures are difficult to achieve so because safety of IoT will be linked to many important scenarios of future 5G. Automata theory was used in this study to address the enormous heterogeneous IoT networks. One of the methods proposed here extends Labelled Transitions Systems to describe IoT systems uniformly in order to detect intrusions by comparing the activity flows between them[25].

The study developed a method for detecting intrusions, created event databases, and put the Events Analyzer to work on real-world cyberattacks. In this case, even advanced processes like standard machine-learning algorithms had difficulties recognising even minor mutations of attacks over time.

In the context of IoT, privacy preservation and intrusion detection are both more difficult and more complicated, as demonstrated by Gunupudi et al. [28]. With the aim to describe each high dimensional sample of the global dataset by an analogous approach with reduced dimensions in this work, membership functions were developed to group attributes of the global dataset progressively. Using dimensionality reduction techniques, a simplified representation of the data was created that may be utilised as input for classifiers[18][19].

Based on software-defined networking, Flauzac et al. [29] proposed IoT security designs (SDN). The SDN-Domain is a type of SDN-based architecture that can be used with or without infrastructure. The suggested architecture was presented in detail and the advantages of using SDN were summarised. Ad-hoc access network control and global traffic monitoring were examined in this article, as well as certain architectural design options for SDN utilising OpenFlow and the performance consequences of those choices were pointed out and debated.

III. FEATURE OPTIMIZATION BY DISTRIBUTION DIVERSITY

The method portrayed is a machine learning approach that functions in sequence of learning and detection phases. The objective of the proposal is to defend intrusion practices that are switching by the external networks linked to the target IoT network. The learning phaseof the proposed method uses the given records of the network transactions that are labeled either as positive or negative, which indicates the prone to intrusion or not in respective order. Further, the learning phase applies set theory and identifies the all possible unique subsets of the attributes, which are representing the values in the given network transactions fall in either of the class label positive or negative. Further, these subsets are sorted in ascending order of their size. Afterwards, for each of these subsets, the values projected in different network transactions both class labels are collected as set such that, each entry of this set is the pattern of values representing attributes of the corresponding subset. Later, the learning phase verifies the significance of these patterns towards the records of both labels.

It's done statistically by calculating the difference between the distribution of positive and negative values for a set of qualities. Attribute patterns with a greater gap between their corresponding patterns of values derived from records labeled as positive and those acquired from those records labeled as negative are shown to be optimum for training classifiers. In regard to measure the distance, we opted to the statistical method called dice similarity coefficient.

A. The Features

The features used by the training phase of the proposed method DDMFO are the pattern of values projecting the pattern of attributes. In this regard, the phase that determines the features as follows.

Let the given set NT of network transactions that are labeled either as positive or negative, which represents either prone to intrusion or not in respective order. Find the attributes as a set A, which are representing the values of each record $\{r \exists r \in NT\}$ of the set NT .

Find all possible unique subsets of the attributes listed in set A, which are listed as set AS , such that each entry of the set AS is the unique subset $\left\{s \exists s \in AS \wedge s \subset A\right\}$ of the set A. Let the map F , which is having a set VS that mapped by a subset $\left\{s \exists s \in AS \wedge s \subset A\right\}$ and the each entry $\left\{e \exists e \in VS \wedge e \in r\right\}$ of the set VS is the set of values projected in each record $\{r \exists r \in NT\}$ for the attributes of the corresponding subset s. Hence, an entry $\{s \rightarrow VS\}$ in the map F is the key s value VS pair, here the value VS is a set, and each entry e of this set VS is the pattern of values representing the attributes found in key s in the corresponding sequence of attributes.

Further, performs the following to enable the dice similarity coefficient can identify the optimal features from the map F

- For each entry of the map F having subset s of the attributes A as key, Begin
    - let the set VS that mapped to key s,
    - List unique entries of the set VS as set UVS
    - Add the subset s and set UVS as key and value pair to the map UF
- End
- Let partition the records given as input to training phase in to sets NT^{+}, NT^{-} such that these sets represents the records that are labeled as positive and negative in respective order.
- For each subset $\left\{s \exists s \subset A\right\}$ Begin
    - For each set $\left\{UVS \exists \{s \rightarrow UVS\} \in UF\right\}$ that mapped to set s as key in map F
        - For each record $\left\{r^{+} \exists r^{+} \in NT^{+}\right\}$ of the set NT^{+} Begin
- Move the index i of an entry $\left\{e \exists e \in UVS \wedge e \in r^{+}\right\}$ that exists in both in set UVS and record r^{+} to the set V_s^{+} .This is the index of "pattern of values" in set UVS representing the attributes of the set s in record r^{+}
        - End
        - For each record $\left\{r^{-} \exists r^{-} \in NT^{-}\right\}$ of the set NT^{-} Begin
- Move the index i of an entry $\left\{e \exists e \in UVS \wedge e \in r^{-}\right\}$ that exists in both in set UVS and record r^{-} to the set V_s^{-}. This is the index of "pattern of values" in set UVS representing the attributes of the set s in record r^{-}
        - End
    - End

B. Dice similarity coefficient

For the sake of determining whether or not the two vectors provided are diversified, this model adaption is seen as critical. In order to detect two different values from the same distribution, the known statistics suggest that a high dice similarity coefficient should be used. The 's Similarity Coefficient is customized to choose the best features for the training set's positive and negative label records using the Dice Similarity Coefficient. The following equation can be used to determine the Dice Similarity Coefficient when two vectors have a wide range of values.

$$dsc = \frac{2^{*} | v_1 \bigcap v_2 |}{| v_1 | + | v_2 |}$$

In the equation above

$| v_1 |, | v_2 |$ Denotes the cardinalities of the corresponding vectors v_1, v_2, and the notation $| v_1 \bigcap v_2 |$ denotes the cardinality of the intersecting values of the given vectors v_1, v_2

If the observed dice similarity coefficient between the two vectors is less than the specified dice similarity coefficient threshold, it indicates that the given vectors are distinct. $dsct$ (usually $0.7 \leq dsct < 1$).

C. Optimal Feature Selection

The features selected from the network transactions given as input to the training phase are listed as the sets $\left\{V_s^+ \exists s \subset A\right\}, and \left\{V_s^- \exists s \subset A\right\}$ for each subset of attributes. The dice similarity coefficient is used further to identify the distribution diversity between the respective set $\left\{V_s^+ \exists s \subset A\right\}, and \left\{V_s^- \exists s \subset A\right\}$, and if diversity observed then the subset s represented by the values from positive and negative records of the training set is considered as optimal to classify the unlabelled network transactions.

D. Class Label Assessment

For given set of test records, each record t is being processed, which extracts the pattern of values for all possible subsets of exists in the set AS . Further, the probability of both class labels for each of the corresponding patterns will be estimated. Then, the fitness of the provided test record toward the affirmative label will be calculated, which is the difference between the mean of the probabilities discovered for all of the related patterns toward the positive label and the departure error. Similarly, the fitness of the given test record towards negative label also being estimated. This is the absolute difference of the average of the probabilities identified for all of the corresponding patterns towards negative label and their deviation error.

Further, the test record will be labeled as positive, if the fitness of the corresponding record t towards positive label is greater than the fitness of the corresponding record t towards the negative label. If not, the fitness of the record towards the negative label is greater than the fitness of the record towards positive label, and then the record will be labeled as negative. In other case, if both fitness values respective to positive and negative labels are approximately equal, then the record will not be labeled and recommended for administrative decision.

IV. Evaluation & Results

An IoT sentinel comprises of million records approximately which are labeled as positive (prone to intrusion) or negative (not intrusion). The experimental study is carried on dataset named IoT Sentinel. For the experimental study, amid million record, 190000(negative: 90000, and positive: 100000) records are taken into consideration. The learning phase of the proposed model DDMFO is trained with the75% of the positive and negative label records among the given input dataset were used. Therest 25% of positive and negative records were used to assess the performance of the classification process in regard to accuracy and false alarming. The inputs given and outcomes obtained for the different statistical metrics often used in classifier performance assessment are listed in table1.

TABLE 1: Label prediction phase inputs and outcomes

Positives (training)	75000
Negatives (training)	67500
Positives (testing)	25000
Negatives (testing)	22500
True Positives	22558
True Negatives	20070
False Positives	2430
False Negative	2442
precision	0.903
Negative Predictive Value	0.892
Accuracy	0.897
Sensitivity	0.9023

Specificity	0.892
False Positive Rate (Fall-out)	0.0977

The suggested model utilizes 47500 (benevolent: 22500, and malevolent: 25000) records in prediction stage. The accurately predicted records were 44541 from the outcomes of predictive analysis. Amid these 19853 are accurately labeled as negative. And 24688 are accurately labeled as positive. Therefore sensitivity which is defined as "true positive rate" is 0.9023(It is the ratio of true positives (TP) contrary to actual positives), and the specificity which is defined as "true negative rate" is 0.892 (It is the ratio of true negatives (TN) contrary to actual negatives). And 2959 records is the amount of falsely predicted records. Amid these, the total number of falsely labeled records is 2647 which are considered as malevolent (positive), and the total number of 312 falsely labeled records is considered as benevolent (negative).

The "positive predictive value" is 0.903 (It is the ratio of TP against aggregate of TP and FP), and "negative predictive value" is 0.892 (It is the ratio of TN against the aggregate of TN and FN). And 0.897 is the complete predictive accuracy that is ratio of aggregate of TP and TN against to the amount of records utilized in predictive analysis. The analysis reveals that the suggested heuristics to measure the malevolent and benevolent extent of IoT network dealings are significant to distinguish IOT network traffic defined as malevolent and benevolent with an accuracy of 89.7%. The represented sensitivity of the suggestion (sensitivity: 90%) signifies that miss rate is low. Since the specificity is approx., 89%, fall out is also considerably high, which is 9%. In the Figure 1, the metric values are shown:

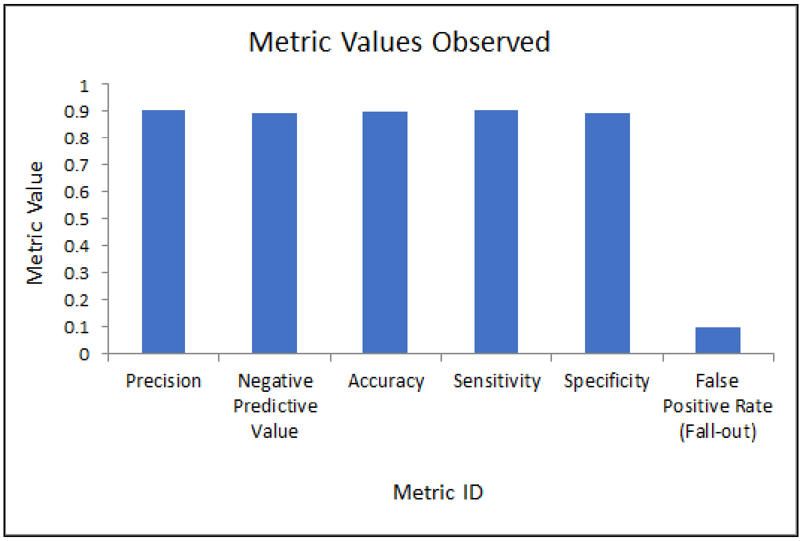

Figure 1: The experimentally determined metric values

V. CONCLUSION

Proposed system is a feature selection and optimization technique that built over the statistical method called Dice similarity Coefficient. The proposal is intended to select optimal features from the set of IoT network transactions labeled as positive or negative to prone the intrusion practices. To improve the classification performance that portrays the provided Network infrastructure transaction that is susceptible to intrusion or not, the contribution is substantial and robust. The output of the proposed model is scaled through the classifier called naïve Bayes. The Experimental investigation points out that the suggested method is highly significant. However, the false positive rate of benevolent record forecast is generally very high. On the other hand Extreme protection against intrusion inside sensitive IoT networks can be tolerated.

REFERENCES

1. King J, Awad AI (2016) A distributed security mechanism for resource-constrained IoT devices. Informatica (Slovenia) 40(1):133–143.
2. Weber M, Boban M (2016) Security challenges of the internet of things. In: 2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). IEEE, Opatija. pp 638–643
3. Gendreau AA, Moorman M (2016) Survey of intrusion detection systems towards an end to end secure internet of things. In: 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud). IEEE, Vienna. pp 84–90
4. Kafle VP, Fukushima Y, Harai H (2016) Internet of things standardization in ITU and prospective networking technologies. IEEE Commun Mag 54(9):43–49
5. Zanella A, Bui N, Castellani A, Vangelista L, Zorzi M (2014) Internet of things for smart cities. IEEE Internet Things J 1(1):22–32
6. Ayoub W, Mroue M, Nouvel F, Samhat AE, Prévotet J (2018) Towards IP over LPWANs technologies: LoRaWAN, DASH7, NB-IoT. In: 2018 Sixth International Conference on Digital Information, Networking, and Wireless Communications (DINWC). IEEE, Beirut. pp 43–47.
7. C. Gomez, A. Arcia-Moret, and J. Crowcroft, "TCP in the Internet of Things: from ostracism to prominence," IEEE Internet Computing, vol. 22, no. 1, pp. 29-41, 2018.
8. M. Conti, A. Dehghantanha, K. Franke, S. Watson, Internet of things secu- rity and forensics: challenges and opportunities, Future Gener. Comput. Syst. 78 (2018) 544–546. [Online]. Available: http://www.sciencedirect.com/science/ article/pii/S0167739X17316667.
9. T. Mehmood, H.B.M. Rais, Machine learning algorithms in context of intrusion detection, in: 3rd International Conference on Computer and Information Sci- ences (ICCOINS), IEEE, 2016. [Online]. Available: https://doi.org/10.1109/iccoins. 2016.7783243.
10. M.H. Bhuyan, D.K. Bhattacharyya, J.K. Kalita, Network anomaly detection: methods, systems and tools, IEEE Commun. Surv. Tut. 16 (1) (2014) 303–336. [Online]. Available: doi: 10.1109/surv.2013.052213.00046.
11. Ganesh, D., and M. Sunil Kumar. "Improving Network Performance in Wireless Sensor Networks: A Survey." Int. J. Web Technol 5, no. 1 (2016).
12. Ganesh, D., Sunil Kumar, M., & Rama Prasad, V. V. (2017). Mutual Trust Relationship Against Sybil Attack in P2P E-commerce. In Innovations in Computer Science and Engineering (pp. 159-166). Springer, Singapore.
13. Kumar, T. P., & Kumar, M. S. (2021). Efficient energy management for reducing cross layer attacks in cognitive radio networks. Journal of Green Engineering, 11, 1412-1426.
14. P. Sai Kiran et.al, "Power aware virtual machine placement in IaaS cloud using discrete firefly algorithm." Applied Nanoscience (2022): 1-9.
15. Ganesh, Mr D., M. Tech, M. Sunil Kumar, and VV Rama Prasad. "IMPROVING NETWORK PERFORMANCE IN WIRELESS SENSOR NETWORKS." Integrated Intelligent Research (IIR), International Journal of Web Technology 5, no. 01 (2016): 58-61.
16. Harika, A., M. Sunil Kumar, V. Anantha Natarajan, and Suresh Kallam. "Business process reengineering: issues and challenges." In Proceedings of Second International Conference on Smart Energy and Communication, pp. 363-382. Springer, Singapore, 2021.
17. Davanam, G. et.al 2021. Novel Defense Framework for Cross-layer Attacks in Cognitive Radio Networks. In International Conference on Intelligent and Smart Computing in Data Analytics (pp. 23-33). Springer, Singapore.
18. Balaji, K. "Load balancing in cloud computing: issues and challenges." Turkish Journal of Computer and Mathematics Education (TURCOMAT) 12.2 (2021): 3077-3084.
19. Sangamithra, B., P. Neelima, and M. Sunil Kumar. "A memetic algorithm for multi objective vehicle routing problem with time windows." In 2017 IEEE International Conference on Electrical, Instrumentation and Communication Engineering (ICEICE), pp. 1-8. IEEE, 2017.

20. Balaji, K., Kiran, P. S., & Kumar, M. S. (2020). Resource aware virtual machine placement in IaaS cloud using bio-inspired firefly algorithm. Journal of Green Engineering, 10, 9315-9327.
21. Prakash, K. J. (2019). Internet of things: IETF protocols, algorithms and applications. Int. J. Innov. Technol. Explor. Eng, 8(11), 2853-2857.
22. Malchi Sunil Kumar et.al. "Optimised Levenshtein centroid cross-layer defence for multi-hop cognitive radio networks." IET Communications 15, no. 2 (2021): 245-256.
23. T. Pavan Kumar et.al, "Multiple Nash Reputation Cross Layer Classification Framework For Cognitive Networks",Journal Of Mechanics Of Continua And
Mathematical Sciences, Vol.-15, No.-8, August (2020) pp 355-367
24. A.A. Diro, N. Chilamkurti, Distributed attack detection scheme using deep learning approach for internet of things, Future Gener. Comput. Syst. 82 (2018) 761–768. [Online]. Available: http://www.sciencedirect.com/science/article/pii/ S0167739X17308488.
25. J. Granjal, E. Monteiro, J.S. Silva, Security for the internet of things: a survey of existing protocols and open research issues, IEEE Commun. Surv. Tut. 17 (3) (2015) 1294–1312 [Online]. Available, doi:10.1109/comst.2015.2388550.
26. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash, Internet of things: a survey on enabling technologies, protocols, and applications, IEEE Commun. Surv. Tut. 17 (4) (2015) 2347–2376 [Online]. Available, doi:10.1109/ comst.2015.2444095.
27. M. Lopez-Martin, B. Carro, A. Sanchez-Esguevillas, J. Lloret, Conditional vari- ational autoencoder for prediction and feature recovery applied to intrusion detection in IoT, Sensors 17 (9) (2017) 1967 [Online]. Available, doi:10.3390/ s17091967.
28. R.K. Gunupudi, M. Nimmala, N. Gugulothu, S.R. Gali, Clapp: a self constructing feature clustering approach for anomaly detection, Future Gener. Comput. Syst.74 (2017) 417–429. [Online]. Available: http://www.sciencedirect.com/science/ article/pii/S0167739X16308718.
29. G.C. Flauzac O., F. Nolot, New security architecture for iot network, Procedia Comput. Sci. 52 (Supplement C) (2015) 1028–1033.